HACKER JOURNAL

Ci sono molte novità all'orizzonte di HJ. Come prima cosa va rilevato che siamo arrivati al numero 3, ergo continuiamo ad esistere. Poi vi devo annunciare, ma già lo saprete, che ora siamo quattordicinali e forse questa è una diretta conseguenza del primo dato: non solo esistiamo, ma funzioniamo. Ce lo testimoniano le centinaia di lettere di approvazione che riceviamo. La sensazione è che forse siamo riusciti in un piccolo miracolo: abbiamo riunito, se non tutti, una parte sostanziale degli umori così multiformi e variegati della comunità underground. Il secondo miracolo è che la comunità stessa ci ha manifestato il suo appoggio. Miracolo numero 3 abbiamo avvicinato al mondo informatico, spesso un po' stantio e noioso, anche un pubblico nuovo fatto di persone che prima d'ora non avevano mai comprato una rivista di informatica.

Ma ora vi lascio: dobbiamo chiudere il prossimo numero... miracolo numero 4.

bomber78@hackerjournal.it

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. Parola di hackers. SCRIVETE!!!

Anno 1 - N. 3 luglio 2002

Boss: theguilty@hackerjournal.it
a cura **di Servizi Editoriali**
Director: rayuela@hackerjournal.it
Editor: bomber78@hackerjournal.it
Technical editor: caruso_cavallo@hackerjournal.it
Graphic designer: gfag8@hackerjournal.it
Contributors: cronopio@hackerjournal.it (images), Jacopo Bruno (cover picture), Daniele Festa

Publisher
4ever S.r.l.
Via Torino, 51
20063 Cernusco sul Naviglio
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA. - 00187 Roma - Piazza Colonna, 361- Tel. 06.69514.1 r.a./20134 Milano, via Cavriana, 14 - Tel. 02.754117.1 r.a.

Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile: Luca Sprea

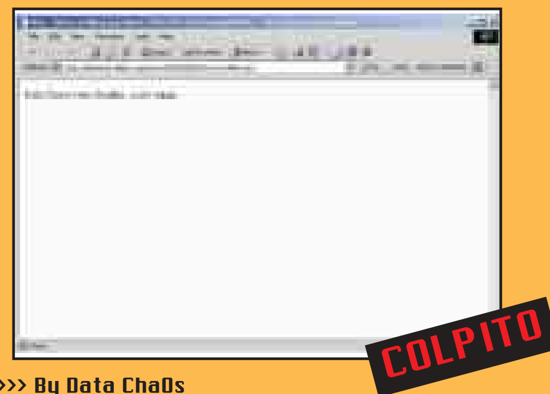
hack•er (hãk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

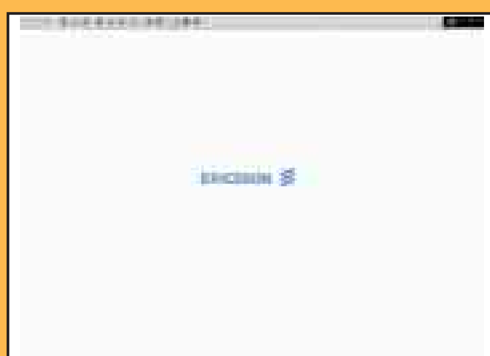
Danni in rete

(gli attacchi in tutto il mondo)

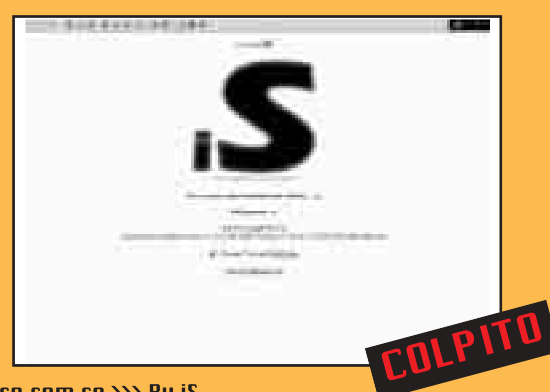




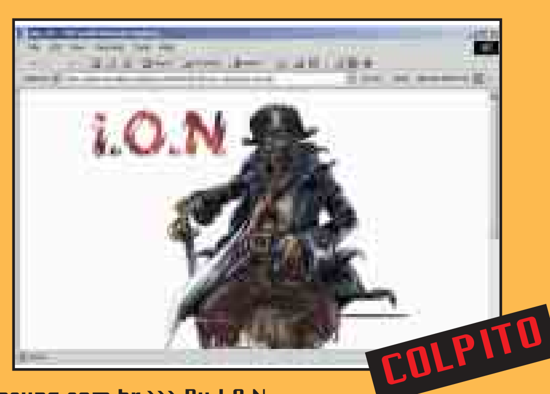
Fuji Film Belgique >>> By Data ChaOs




Ericsson / www.ericsson.ee

Texaco / www.texaco.com.co >>> By iS

Samsung Bresil / www.samsung.com.br >>> By I.O.N.

SPAM ?.........NOOO GRAZIE!!!



La diffusa pratica dello spamming, ovvero l'invio generalizzato di e-mail a un indeterminato numero di destinatari, è stata oggetto di una storica decisione dell' Autorità Garante.

In data 26.03.02, infatti, il Prof. Rodotà ha ordinato a una società, che inviava e-mail pubblicitarie senza consenso, di cessare il comportamento illegittimo e di astenersi con effetto immediato da ogni ulteriore trattamento dei dati, condannando inoltre la società resistente al pagamento delle spese e dei diritti del procedimento direttamente al ricorrente (250 euro).

La normativa di riferimento è la legge n. 675 del 1996 intitolata "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", che all'art. 11 dispone che "il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato...... Il consenso è validamente prestato solo se è espresso liberamente, in forma specifica e documentata per iscritto, e se sono state rese all'interessato le informazioni circa... l'utilizzo e la conservazione dei relativi dati". Una disposizione ben chiara e precisa, ma di fatto per lungo tempo ignorata e aggirata facendo riferimento al successivo articolo 12 della stessa legge, che esclude la necessità del consenso quando il trattamento riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque. E' stato necessario un ulteriore intervento dell'Autority, il quale ha precisato che "gli indirizzi e-mail possono essere raccolti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque", come recita l'art. 7, comma 5-ter, ma non possono essere ricavati da pagine web, gruppi di discussione o altre fonti simili.

Dunque l'attività vietata dal Garante non è il mail spamming, ma il mail grabbing, cioè il rastrellamento indiscriminato di indirizzi e-mail sparsi nella Rete.

L'Italia ha adottato il sistema dell' OPT-IN per cui deve essere il titolare dell'e-mail a dare espresso consenso al trattamento dei suoi dati, anche se in molti altri paesi ancor oggi sopravvive l'opposto sistema dell' OPT-OUT per cui deve essere il titolare dell'e-mail a richiedere la cancellazione dei suoi dati.

Ma chi ci tutela??????............IL GARANTE!!!!!!!!!!!!!!

All'art. 29 della legge sulla tutela dei dati personali è espressamente e dettagliatamente prevista la possibilità di ricorrere al Garante. Dapprima diffidiamo (raccomandata A/R) l'autore dell'e-mail incriminata a cessare dalla sua attività di "spammingaggio" e poi, dopo almeno cinque giorni dalla ricezione della raccomandata inoltriamo un bel ricorso al Prof. Rodotà con le relative prove allegate (STAMPARE SEMPRE L'E-MAIL INCRIMINATA) , il tutto con una spesa di circa 25 euro (tasse comprese!). Il tutto va inviato a: AUTORITA' PER LA GARANZIA NELLE COMINICAZIONI, VIA DELLE MURATE 25, 00187 ROMA. La scellerata società che ci vuole necessariamente informare sulla convenienza delle sue offerte rischia pesanti sanzioni oltre a dover risarcire il danno prodotto ai destinatari delle fastidiose e-mail che hanno presentato regolare ricorso. Inoltre troverebbero applicazione anche le sanzioni previste dal D.L. 185/99 che, limitando le comunicazione a distanza fatte al consumatore, prevede sanzioni pecuniarie sino a cinquemila euro e nei casi più gravi sino al doppio!!!!!!!

Dott. Gaetano Mario Pasqualino
Il cugino7@yahoo.it

Carissimi redatori di Hacker Journal: dopo aver letto la vostra rivista mi sono venute in mente 2 domande: 1) nella rivista spiegate molto bene quali sono le tecniche che un hacker può saper fare, e date anche link dove trovare tutto ciò che gli serve per mettere in pratica ciò che ha imparato: in Italia questo è legale o illegale? 2) Nella rivista verrà messa anche una sezione dove ci saranno le mail dei lettori?

Lungi da noi l'idea di stimolare l'illegalità. La nostra intenzione è quella di informare, di dare strumenti per capire questo mondo sconosciuto ai più, ma estremamente intrigante. Nulla è pericoloso in assoluto, tutto può essere però dannoso se usato nel modo sbagliato. Se pensate, ad esempio, che un PC non sia un oggetto pericoloso, provate a buttarlo giù dal quinto piano e centrare un passante...

Attenzione!!!

Alla url di del nostro sito: http://www.hackerjournal.it/secret-zone è disponibile una sezione riservata solo ai lettori di HJ, per accedere bisogna autenticarsi digitando le seguenti user e password:

user: ml9xe

pass: wks11

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

NEWBIE — MID HACKING — HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).



Ciao, senza volervi buttare giù, vi dico apertamente che mi aspettavo qualcosa di più. Ok, ok, non vi preoccupate questo non è uno dei soliti messaggi di critica... però il livello di informazione va aumentato! Ho seguito la chat del sito e... altra delusione: poca gente che si occupava di sicurezza informatica (a parte XenT con il quale ho avuto uno scambio di idee) la maggior parte dei chatter parlava di "sciocchezze". "Buttatevi" su articoli più tecnici perché secondo me questa rivista è sicuramente indirizzata ad un utenza medio-alta. Ciao a tutti,

Albatross

P.S. Forza e coraggio...

Prendiamo come lettera di critica costruttiva quella di Albatros. L'articolo che ci hai spedito va più che bene: tutti i contributi dei lettori risultano importanti per fare crescere la rivista... Cercheremo di essere più tecnici, speriamo che in questo senso "la forza sia con noi".

La "Music hackering"



"La mattina mi alzo, dopo una rinfrescata faccio colazione e mi dirigo a lavoro. Oggi orario pieno, stracco fino alle 20:00. Torno a casa, un bacio a mia moglie, lei è stanca va a coricarsi. Sarà perchè quei calzini da uomo a terra non sono i miei; ma non ho voglia di discutere su tutto l'intimo uomo che ho sempre trovato ogni volta ch'ho fatto lo straordinario. Ora è quasi arrivato il momento , vado nella sala dove ho il mio fedele PC!. Non ce la faccio più a vederlo spento. Ecco ora lo accendo... dai dai, avanti!!! OOOH questo bip del PC speaker è qualcosa di desolante...
Dai Windows, avviati fammi sentire il tappeto sonoro del desktop, dai sto fremendo, non ce la faccio, forza daiii SIIIIIIIIIIIIII" Salve a tutti, certamente avrete intuito che il tipo dell'intro sopracitata è probabilmente uno dei modelli più noti di utente PC.
Ma è possibile che il computer possa provocare reazioni catartiche così intense da far inghiottire tutte le sofferenze di una giornata e, davanti ad un monitor, renderle gustabili addirittura? Certo è che non voglio fare di tutta l'erba un fascio poiché non è così facilmente catalogabile una situazione del genere; ma anche volendoci apportare delle modifiche (magari di carattere matrimoniale:-) , riferendoci ancora all'episodio introduttivo, rimane sempre un processo consequenziale e regolare per tutti gli utenti Windows:

UTENTE-->ACCENSIONE-->BIP-->AUTO-CONFIG SO-->DESKTOP-->SUONO D'AVVIO.
e non potrebbe mai essere:
PC-->ACCENSIONE-->UTENTE-->SUONO D'ARRIVO DI SIRENA DELLA NEURO.

Io vi invito a riflettere su cio', e soprattutto a non fidarvi di voi stessi. Music Hacking è disciplina analitica. Si tratta di esaminare ogni sorta di suono passante per i timpani (prima che, incosciamente, arrivi al cervello), sviscerarne la composizione e rendere "falla" l'elemento che identifica quella determinata musica come scopo persuasivo, emotivo, rincoglionitivo. **Immaginate un trojan (come brano musicale o suono) che entra dentro voi infettando il corpo; il server (il compositore del brano) potrà fare di voi ciò che desidera.** Forse non è chiaro che oggi la musica, come mass-media, è il più sottile strumento di subdole comunicazioni nascoste tali da condizionarci a fare ciò che non desideriamo o ciò che amiamo ma non sotto il nostro controllo, e solo capendone le funzioni potremmo usare ed "abusarne"... Ritornando al nostro utente "cornuto", come potremmo omettere ,nelle cause della sua calma illogica, il suono d'apertura di Windows? Avete mai assistito ad un avvio multiplo di più Pentium, in qualche azienda o in ufficio? Se tutti sono impostati da predefiniti, avranno lo stesso suono... Beh sembra di stare in paradiso, e non si riesce neanche a distinguere l'inizio o la fine proveniente da ogni fonte di suono. A cosa mira la Microsoft? The Microsoft Sound.wav, di cui stiamo parlando, non ha tale nomenclatura a caso. Il file è composto con una dinamica di volume ascendente, il che crea indubbiamente un senso di decollo, ma che non arriva mai a troncarsi, poiché una volta all'apice, il suono si distribuisce in tante particelle appena percettibili, scomparendo del tutto. Come lo smaterializzarsi di un velo che prima non ci permetteva di guardare l'orizzonte. L 'armonia , vista la presenza di più suoni (o accordi non di tensione, ma di rilassamento) sovrapposti, è usata a soli scopi di immettere tranquillità paradisiache agli utenti. Tutto ciò è solo uno dei tanti impianti di una struttura musicale che abbraccia la maggior parte degli utenti, almeno in italy, mettendosi in condizione di creare nell' interagente (il nostro cornutone) una sorta di pazienza fittizia, caratterizzata dall'appoggio emotivo di tale musica. **Bisogna smettere di essere "rimbambiti informatici" o "mediatici" , bisogna aprire le orecchie, e capire quando perdiamo il controllo della realtà...eccovi la MUSIC HACKING...era un introduzione...vi state chiedendo se siamo in possesso di una scientificità?** La risposta è sì....anzi SI'!!! Ma ne parleremo prossimamente. Intanto cominciate a "sentire" i suoni dei programmi, o degli ipertesti o dei Pop-up, con un "ottica" differente...

PS:<e se c'è qualche richiesta,perché no?>
bye

Ci ha bu

Finalmente anche in Italia è arrivata in edicola una rivista del settore non nascosta in qualche sito Underground !! Volevo segnalare il sito che da alcuni mesi cerchiamo di tenere al meglio possibile anche se il tempo per lavorarci è molto poco.Vi auguro molta fortuna !!! E. Palena e il team di Napolifirewall.com

LA FORZA DELL'INDIPENDENZA: NIENTE PUBBLICITÀ

Ciao a tutti, ho comprato il primo numero del journal, ecco quello che non mi é piaciuto...
1. Troppe news... su 30 pagine di giornale 7 sono di news... e solo 3 articoli riguardano l'hacking
2. Una impostazione ampiamente "microsoftiana", dal momento che non c'é un solo nome di programma linux ma ce ne sono di programmi windows... E poi questa impostazione é dimostrata dal fatto che nel sondaggio sul sito "quale sistema di file sharing preferisci" ci sono solo sistemi per windowsiani.
3. Poco spazio all'hacking vero e proprio
4. Piccole fesserie dette a riguardo dei macintosh e della ricerca di warez. Gli utenti mac, almeno fino al mio ultimo contatto con uno di loro, usano le hotline.
Per il resto il secondo numero lo compro così do in giro la password della secret area a tutti quanti e vedo se magari togliete tutta quella pubblicità (scherzo, questa di non avere pubblicità é una cosa che mi ha veramente colpito, bravi!).
E poi la storia di avere un server su cui fare pratica (e magari sfide e tornei) é una bellissima idea e credo mi farà restare dei vostri...
Ciao

Nick

Il sondaggio on-line riguarda il sistema file sharing preferito. Al momento è in testa purtroppo Winmx, del caro buon vecchio zio Bill. Auspichiamo un cambio di rotta da parte di tutti i partecipianti...



Salve sono Nazzareno Schettino. Ho realizzato e gestisco il sito NoTrace.it vorrei chiedervi se potreste pubblicare unasegnalazione di http://www.notrace.it sul vostro giornale come ho visto che avete fatto per altri siti!

Accontentato!

AIUTO: VERICHIAMO INSIEME GLI URL!

Ciao a tutti, complimenti per la rivista e naturalmente posseggo la numero 1 (come la moneta di Zio Paperone) speriamo che mi porti fortuna ;-). Ora finita la parte di lecchinaggio :-) passiamo al dunque , vi volevo solo segnalare il mio sito web www.piratiassociati.org.
Poi vi volevo segnalare che nella Vostra home page avete fatto un errore clamoroso di battitura http://www.hackerjournal.it/Home.htm alla voce NEWS avete scritto clicca con 2 L
ASINI!!!! :-)))))))))))))
ciao

Per il sito tutto fatto per quanto concerne la home: gasp, hai ragione, abbiamo provveduto ad infilare il berretto a punta dei somari e ci siamo posizionati dietro-la lavagna, contento?

Non ho trovato la pagina per scaricare il programma all'indirizzo che avete pubblicato. Come mai, dove ho sbagliato? PS come posso controllare se sto navigando in anonimato dopo aver installato ANONYMITY 4proxy?
Grazie

Guido

Se gestisci un sito puoi visitarlo e guardare nel quadro di amministrazione, altrimenti ti fidi... Comunque tranquillo... funziona!

Complimenti per la rivista. Vorrei segnalarvi il mio sito:
http: //it.geocities.com/sistem743.
Poi ho letto sul primo numero che forse aprirete un server su cui provare varie tecniche per hackerarlo.
Questa idea mi ha colpito molto e penso che sarebbe molto utile, e quindi vorrei chiedere se questo progetto sarà realizzato. Infine, la mia ultima domanda è: corro pericoli a gestire un sito dedicato all'hacking?
Grazie

Sì rispondiamo a te, ma idealmente a tutti i lettori che ce lo chiedono: Gymnasium partirà, non è una bufala... ci stiamo organizzando, del resto non è un progettino "da niente" e vogliamo fare le cose perbene.

Salve redazione di HJ, vi scrivo questa mail in merito ad unlink, come avrete colpito dall'oggetto. Io sono il webmaster di http: //pincopall.cjb.net o se preferite pincopall.ontheweb.it che almeno non fa apparire nessun pop.up, ora, tale sito è un sito-archivio, lo vedrete se vorrete visitarlo, ed è la più grande raccolta d'Italia, e credo anche d'Europa , di tutorials in italiano ed in inglese circa il reverse-engineerin ed il cracking (di software) e preacking. Saluti
Pincopall

Ciao a tutto lo staff di Bismark vorrei che inseriate il mio link nella rivista HACKER JOURNAL ve ne sarei molto grato. Il mio url e www.w3x.cjb.net <http://www.w3x.cjb.net> spero accettiate...

Detto , Fatto!!!

HOT!



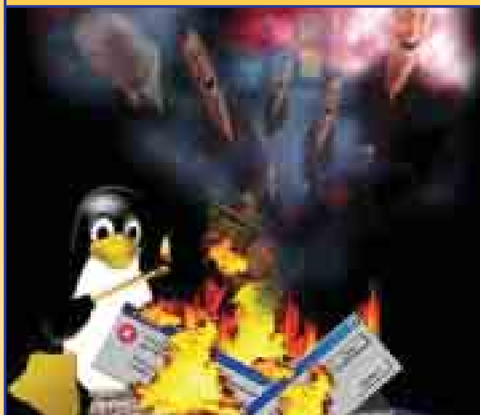
I SEGRETI MILITARI SI TROVANO SU INTERNET

Wargames va in onda su internet: secondo l'autorevole quotidiano "Kronenzeitung", un diciassettenne austriaco avrebbe intercettato via Internet diversi segreti militari americani che riguardano in particolare i dettagli sul recente **accordo tra Stati Uniti e Russia per il disarmo nucleare** firmato il 24 maggio scorso a Mosca.
Sembra che il ragazzo cercasse pagine Internet riguardanti informazioni militari quando sul suo schermo sono comparsi improvvisamente documenti segreti del ministero della Difesa degli Stati Uniti. Poco dopo pare che Robert sia stato contattato da un agente dell'Fbi, che da Washington ha telefonato al ragazzo per chiedergli come avesse fatto ad accedere ai documenti segreti. Alla faccia della tanto sventagliata sicurezza: se fossimo in Bush ci daremmo una toccatina da qualche parte...

IL MUSEO ASSOLDA GLI HACKER

Gli hacker hanno risposto all'appello lanciato dal direttore del centro culturale e museo letterario norvegese che non riesce più ad accedere agli archivi telematici a causa della morte dell'unica persona che ne conosceva la password di accesos e che, naturalmente, non l'aveva mai detta a nessuno. Il direttore del museo Ottar Grepstad ha spiegato a una trasmissione alla radio nazionale norvegese le ragioni che l'hanno indotto a chiedere l'aiuto degli hacker per riuscire a scoprire la fatidica password che finora ha resistito a tutti i tentativi. Grepstad ha raccontato anche che la risposta degli "esperti alternativi" è stata superiore alle sue stesse aspettative. L'archivio inaccessibile del museo, dedicato al famoso linguista norvegese Ivar Aasen, contiene più di 1600 libri e documenti di grande interesse per gli studiosi.

LINUX UBER ALLES: ZIO BILL AL TAPPETO...



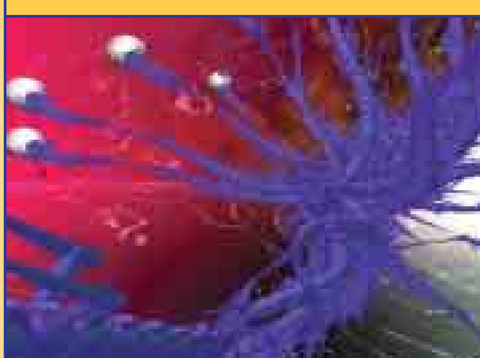
Da Francoforte giunge una notizia di per sé clamorosa. Il Governo tedesco ha deciso di ridurre la propria dipendenza tecnologica dai sistemi proprietari di Microsoft, una decisione suggellata da una importante partnership con IBM per portare sulle infrastrutture della Pubblica Amministrazione i sistemi open source ed in particolare Linux (vedi intervista numero 1). Il ministro dell'Interno Otto Schily ha dichiarato che l'utilizzo di sistemi basati sull'open source di Linux e non più Microsoft porterà ad un aumento della sicurezza delle infrastrutture telematiche della **Pubblica Amministrazione**, tanto a livello federale che locale. Non sono ancora noti i dettagli economici dell'accordo con IBM, tuttavia Schily ha infatti dichiarato che "il Governo tedesco con questa scelta vuole innalzare la soglia della sicurezza informatica, come dire che con software Microsoft non è che ci sia da stare troppo tranquilli: bella pubblicità.

L'UNIONE EUROPEA INDAGA SULLA MICROSOFT: TEMPI DURI!

Il commissario europeo alla concorrenza Mario Monti sta indagando su irregolarità alle leggi antitrust commesse da Windows, ma ora la Commissione Europea ha messo sotto indagine anche un altro aspetto dell'impero di Bill Gates: la raccolta di dati personali compiuta attraverso il servizio "free.Net Passport". Alcuni europarlamentari sostengono che il servizio sia incompatibile con le norme europee sulla tutela della privacy, visto che consente alla Microsoft di collezionare dati personali di utenti mentre eseguono su Internet una serie di operazioni tra cui l'invio di e-mail attraverso il sistema "hotmail". Insomma Microsoft è una specie di "portinaio" on-line cui nulla sfugge...



KLEZ, UN VIRUS DA GUINNESS



La notizia arriva da MessageLabs, azienda e osservatorio antivirus. Sembra che Klez.H stia prendendo il posto di SirCam tra i virus aggressivi che maggiormente colpiscono gli utenti internet. I dati diffusi dall'azienda parlano di una e-mail infetta ogni 300 che circolano in rete, il che non solo si traduce in una continuativa e diffusissima infezione ma anche **evidenzia la capacità di Klez.H** di resistere alle difese tradizionali e di moltiplicarsi a dismisura.
A quasi due mesi dalla scoperta di Klez questo worm è sempre più diffuso e "popolare". Se si conta non solo Klez.H ma anche le altre varianti di Klez si arriva a cifre davvero impressionanti.
Del resto, ormai i virus sembrano fare parte del corredo di ogni e-mail che si rispetti, come dire: un worm al giorno toglie il PC di torno (vecchio detto popolare).

"PENSO CHE CI SIA POSTO, SUL MERCATO MONDIALE, PER CIRCA 5 COMPUTERS".
> Thomas J. Watson, Amministratore Delegato IBM, 1948.

"MACRO" COME LE CIAMBELLE: COL BUCO



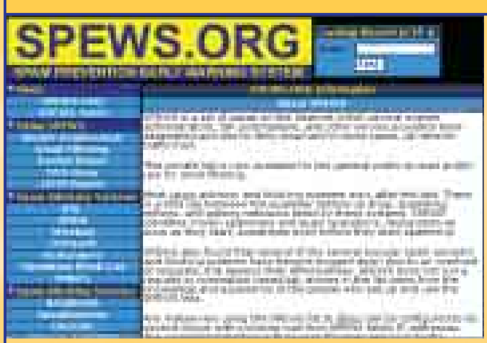
Next Generation Security Software (NGSS) ha scoperto nella versione Windows di JRun 3.1, il server Java 2 Enterprise Edition di Macromedia, una seria falla di sicurezza che potrebbe consentire ad un aggressore di guadagnare, da remoto, il pieno controllo di un sistema. In un bollettino di sicurezza NGSS spiega che la vulnerabilità riguarda tutti i sistemi Windows NT/2000 su cui si trovi installato, insieme a Internet Information Services 4 o 5, JRun 3.1. La falla consiste in un buffer overrun contenuto in una DLL ISAPi installata di default da JRun: un cracker, sfruttando il fatto che in JRun le DLL vengono caricate nello stesso spazio di memoria del servizio Web (inetinfo.exe), potrebbe dunque essere in grado di guadagnare l'accesso al sistema con i massimi privilegi (gli stessi dell'account System).
Il pericolo, secondo alcuni esperti di sicurezza, consiste nella possibilità che qualcuno confezioni **un worm simile a Code Red** in grado di bucare la falla di JRun e infettare i server.
Macromedia, che ha già rilasciato una patch, sostiene che la nuova versione 4.0 di JRun non è afflitta dal problema.

COLLEONIROBERTO.IT ALZA BANDIERA ANARCHICA



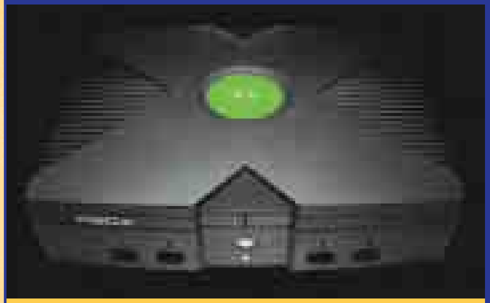
Defacement firmato Anarchy Control sul sito **Colleoniroberto.it.**
Abbiamo fatto in tempo ad immortalare l'operato di AC prima che le cose venissero rimesse a posto. **Niente da dire proprio un bel lavoretto**…

CORNUTO E "CAZZIATO"



Uno dei più simpatici modi di dire trova finalmente un calzante esempio anche in ambito tecnologico. Il "cornuto" è Joseph McNicol che ha denunciato all'autority antispam la società T3 Direct, la cui fama è tale che viene definita da alcuni esperti come "spamhaus".
Quest'ultima di contro ha chiesto circa 45mila euro di danni a McNicol, accusato di aver provocato l'inserimento di T3 Direct nella black list antispam gestita dal celeberrimo **Spews.org**. Quei 45mila sembrano tanti ma T3 ha dettagliato il conto della spesa nella propria denuncia. 8mila sarebbero da imputarsi a danni dovuti al rimpiazzo dei numeri IP bloccati nella lista nera, altri 3mila per l'intervento dei tecnici per la creazione di un nuovo sistema email, 3mila per l'acquisto di un nuovo server e i rimanenti per i mancati guadagni dei 20 giorni in cui l'azienda ha atteso che la propria connettività fosse riattivata. Attorno a McNicol si sta radunando una imponente comunità di utenti e alcune associazioni che sostengono le operazioni antispam.
Quindi attenzione: se qualcuno vi investisse mentre attraversate le strisce pedonali potrebbe anche capitarvi di essere denunciati per danneggiamento di paraurti, così vanno le cose nella stupenda società tecnologica.

HOT!



CRACCATA LA PROTEZIONE DI XBOX: SI GIOCA GRATIS O QUASI…

Xbox sembra non avere più segreti. Questo almeno per Andrew Huang, uno studente del MIT che in questi giorni ha pubblicato un documento (ftp://publications.ai.mit.edu/ai-publications/2002/AIM-2002-008.pdf) in cui sostiene di essere riuscito a craccare il sistema di protezione della console di Microsoft. L'hacker ha spiegato di aver analizzato a fondo il protocollo di sicurezza di Xbox e di essere riuscito, nel giro di pochissmo tempo, solo tre settimane, a "sniffare" la chiave segreta necessaria a legittimare l'esecuzione di un qualsiasi contenuto presente all'interno di un disco. Huang sostiene che la conoscenza di questa chiave rende possibile far girare su Xbox - senza la necessità di interventi sull'hardware - qualsiasi programma: dal software open source ai giochi copiati. La scoperta di Huang arriva in concomitanza con il rilascio dei primi mod-chip per Xbox, chippetti che, andando ad operare direttamente sulla scheda madre della console, promettono di aggirare tutte le barriere protettive e consentire l'esecuzione di software pirata o dischi d'importazione.

DEFACCIATO IL SITO DI PUGLIAONLINE

Non avrà trovato posto in un bungalow sul Gargano, oppure non ha gradito l'olio di oliva caratteristico della regione, fatto sta che un "craccatore mascherato" ha defacciato il sito di Pugliaonline lasciando la sua personalissima firma che vi riportiamo…



HOT!



ASP: ALTO RISCHIO VULNERABILITA’

ASP (**Application Service Provisioning**): sicurezza zero, virgola, zero. E’ come la pensano le aziende italiane sui sistemi che adottano o comunque hanno sentito parlare dei servizi Asp.
Una ricerca condotta presso 220 aziende italiane con più di cinquanta dipendenti ha messo in luce che solo il 39% delle imprese è a conoscenza delle caratteristiche e delle modalità che contraddistinguono un servizio ASP.
Il 12,3% degli intervistati considera i servizi ASP identici a quelli di tipo outsourcing, mentre il 58,2% ne riconosce le differenze.
I rappresentanti delle 220 aziende che rappresentano il campione per la ricerca di Sirmi hanno inoltre sottolineato un problema saliente, da parte dei fornitori ASP, **quello della sicurezza** che non sembra essere uno dei punti di forza del sistema.
Per quanto ci concerne vale la pena di ricordare come il nostro primo sito in .asp sia stato miseramente bucato: che le aziende abbiano ragione?

LA FIAT NON VA PERFINO IL SUO SITO ROTOLA VIA

I problemi per la Fiat proprio non finiscono mai: non vende le macchine, ha una situazione finanziaria che definire delicata è un eufemismo e pure i cracker la prendono di mira. Un sito olandese della casa di Torino è stato ripetutamente bucato, prima da "S4t4n1c_S0uls" e subito dopo per mano di i "**TriaX**" .
Dopo una breve pausa per permetterne il ripristino, che evidentemente non ha risolto i problemi, il giorno successivo i "**S4t4n1c_S0uls**" hanno di nuovo modificato l'home page.

ECHELON NON BASTA: CI SI METTONO ANCHE I “BISCOTTINI” SPIONI…

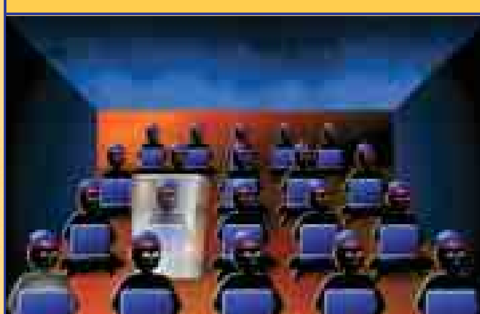

NEWS FOCUS — ECHELON

Super-stickybeak hears all

Use certain words in any kind of electronic communication and you could be subjected to unwelcome attention. European correspondent HELEN McCABE explains

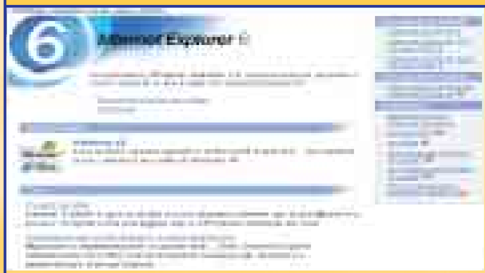
La Scottish Enterprise ha messo a punto una nuova tecnica per farsi “i fattacci nostri”.
Tale tecnica consente di tenere traccia dell'utilizzo di Internet tramite "sensori" che sostituiscono i cookie.
Questa tecnologia può funzionare su qualunque Web server e può monitorare l'uso di Internet in tempo reale. In aggiunta, questo software è in grado di bloccare l'accesso ad alcuni siti, alle e-mail e a diversi tipi di documenti.
Secondo la società questa nuova tecnica dovrebbe servire per il monitoraggio della **navigazione dei dipendenti nell'ambiente di lavoro**, e per permettere ai genitori di controllare in che modo i figli utilizzano Internet.
Evidentemente alla Scottish pensano che siano tutti fessi, altrimenti non avrebbero rilasciato tali dichiarazioni, la sensazione è che la privacy sia un concetto sempre più a rischio e sempre meno soggetto a tutela...

FRAGROUTE: UN PO’ PER CRACKER, UN PO’ PER ESPERTI DI SICUREZZA



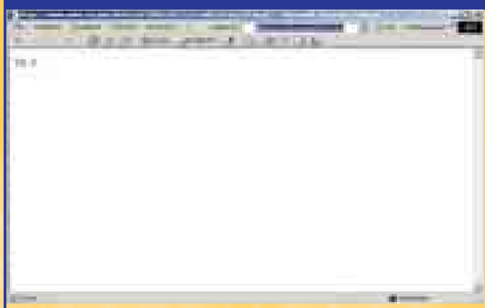
Un nuovo strumento, denominato Fragroute, utilizza alcune tecniche per aggirare i sistemi di riconoscimento basati sulle firme digitali utilizzati da molti sistemi di rilevamento delle intrusioni e dai firewall. Il programma Fragroute **(http://www.monkey.org/~dugsong/fragroute/ - http://www.anzen.com/research/nidsbench/fragrouter-1.6.tar.gzha)** un doppio utilizzo. Evidenzia le deficienze nel sistema di sicurezza di un network, e queste informazioni possono aiutare sia l'amministratore di sistema che deve proteggere la sua rete, sia l'hacker che la vuole attaccare. Il programma sfrutta diversi modi di inserire dati specifici in una sequenza di informazioni, per ingannare i programmi di rilevamento. Funziona così: un comando inviato al server può essere camuffato tramite l'aggiunta di dati estranei e arbitrari. Il server attaccato elimina automaticamente tutti i dati inutili e lascia il comando funzionante, ma dannoso. Molti sistemi di rilevamento delle intrusioni non eliminano invece i dati fasulli, cosicché il comando dannoso resta nascosto e non identificabile dalle funzioni di riconoscimento del sistema e quindi l’attacco funziona lo stesso in barba alle precauzioni antri-intrusione.

UELLA! ANCHE QUESTO MESE IE PRESENTA LA SUA BELLA FALLA



Per la rubrica “Internet Explorer il buco del mese” vi proponiamo una nuova vulnerabilità del browser più bucato della storia (recente) informatica. Questa volta a salire alal ribalta è l’archetipo del World Wide Web, ovvero Gopher il protocollo con cui è nato internet. Explorer ha proprio al suo interno un client Gopher (che gestisce gli URL del tipo gopher://) contenente una pericolosa falla di sicurezza che potrebbe consentire ad un malintenzionato di prendere il pieno controllo del computer vittima. La vulnerabilità, scoperta dalla società di sicurezza Oy Online Solutions (OOS), consiste in un buffer overflow nel codice di IE che gestisce le connessioni Gopher, un bug che può essere sfruttato remotamente da un aggressore per eseguire sulla macchina dell'utente qualsiasi tipo di codice e compiere azioni come la ricezione, l'upload, l'installazione o l'esecuzione di file. La falla sembra interessare tutte le versioni ancora in circolazione di IE, incluse le più recenti come la 5.5 e la 6.0. In attesa del rilascio di una patch da parte del big di Redmond, nel suo advisory OSS spiega come disabilitare il protocollo Gopher da IE.

VIOLATI DUE INDIRIZZI TIN: DITECI COME



Mr. X ha colpito ancora, e questa volta pesantemente: due indirizzi IP appartenenti alla rete di Tin.it (**http://r-mi214-6a236.tin.it** e **http://r-to081-2-474.tin.it**) sono stati violati dal Cracker.
I due server violati contengono rispettivamente:
-un sito per lo scambio di file MP3 e DivX
-un dispositivo basato sull'ambiente operativo Allegro-Software-RomPager, impiegato da diversi prodotti hardware di rete come switch, printer, router e altri. Uno dei metodi che può essere stato utilizzato per violare i siti è legato proprio ad Allegro-Software-RomPager, di cui è nota una vulnerabilità presente nella diffusa versione 2.10, trovatela voi e ditecela! sensibile a particolari richieste HTTP.

BENJAMIN UN BEL WORM PER KAZAA



Le modailità di intrusione di questo worm sono le seguenti:
Una volta installatosi, il worm visualizza un falso messaggio di errore:
- Error Access error #03A:94574: Invalid pointer operation
- File possibly corrupted. [OK]
quindi copia se stesso all'interno della cartella di sistema di Windows (%WinDir%\SYSTEM) come:
- EXPLORER.SCR
Benjamin crea poi due chiavi all'interno del registro di sistema:
-[H_L_M\Software\Microsoft\Windows\CurrentVersion\Run]
-"System-Service"="C:\\WINDOWS\\SYSTEM\\EXPLORER.SCR"
-[HKEY_LOCAL_MACHINE\Software\Microsoft] "syscod"= "0065D7DB20008306B6A1"
in questo modo può autoeseguirsi a ogni riavvio del sistema. Come difendersi? Ancora non si sa.

"I COMPUTER SONO INUTILI. TI SANNO DARE SOLO RISPOSTE".

› **Pablo Picasso**

HOT!!



IL MONDO E' DEI PIRATI!

Un mondo in mano ai pirati, questo è quello che traspare dal rapporto della BSA (Business Software Alliance). Secondo tale studio il controllo sul software proprietario da parte dei produttori sembra sempre più difficile e persino raro, se si considera che il 40 per cento di tutto il software utilizzato sul globo è copiato o utilizzato illegalmente.
Una cifra assolutamente incredibile che fa riflettere su quanto sia forse ormai utopico pensare a contromisure e o rimedi antipirateria, forse bisogna semplicemente accettare la fine del copyright.
Il rapporto della BSA arriva dopo più di un anno di lotta dura su tutti i fronti contro la pirateria industriale, contro la criminalità organizzata e persino contro quei paesi che sono accusati di non contrastare adeguatamente il fenomeno.
A quanto pare, complice Internet e una cultura che non si sposa con quella del copyright ad ogni costo, gli indici di pirateria continuano a crescere un po' dappertutto. In Europa Occidentale la percentuale di software illegale, secondo la BSA, è aumentata del 3 per cento rispetto al 2000, raggiungendo il 37 per cento, cifra cui vengono fatte corrispondere perdite per 2,9 miliardi di euro. Un calcolo che viene realizzato moltiplicando per il prezzo di listino delle licenze il numero di copie di software pirata in circolazione.In questo quadro sorprende positivamente, per la BSA, il fatto che in Italia il tasso sia sceso, sebbene solo dal 46 al 45 per cento. In termini relativi il nostro paese "migliora" di un punto rispetto all'anno precedente nella graduatoria europea degli Stati a maggior tasso di pirateria informatica (quarta tra i "peggiori" anziché terza).

HOT CUP!

"FEBBRE" DA MONDIALI

La febbre in questione non è quella di origine virale, derivante da influenze e malanni di raffreddamento legati agli sbalzi di temperatura, ma quella che il PC può contrarre in seguito all'intrusione di VBS/Chick-F, un worm che si camuffa da applicazione per visualizzare i risultati delle partite del Mondiale in Korea. Il worm arriva attraverso una e-mail che ha per oggetto il testo "RE: Korea Japan Results" e per corpo del messaggio "Take a look at these results... Regards, ". In allegato si trova il file HTML compresso (CHM) che, una volta lanciato, visualizza la stringa di testo "Enable activeX To See Korea Japan results": se l'utente attiva lo script ActiveX, il worm cerca sui dischi un'installazione di mIRC, il noto client di IRC attraverso cui il vermicello è in grado di diffondersi. Come "vizio di famiglia" Chick-F ha quello di spedire se stesso ai contatti della rubrica dell'utente infettato.



SOLARIS BUCATO

È stata riscontrata una vulnerabilita' nel protocollo di stampa di Solaris "in.lpd", in cui un remote user potrebbe eseguire codice arbitrario sul sistema ed avere cosi accesso al sistema con privilegi di root. Le due falle di sicurezza consistono in due buffer overflow contenuti negli agenti software "snmpdx" e "mibiisa", due componenti che fanno parte delle funzionalità SNMP (Simple Network Management Protocol) di Solaris e girano con i privilegi di root. Entrambe le vulnerabilità possono essere sfruttate sia da locale che da remoto e interessano le versioni 2.6, 7 e 8 di Solaris.

Sistemi affetti:
UNIX (Solaris - SunOS)



SGI IRIX "FALLATA"



È stata riscontrata una vulnerabilità in SGI IRIX 'rpc.passwd' , un'utility del sistema operativo SGI IRIX. Un remote user potrebbe sfruttare questa falla per ottenere i privilegi di root.

Sistemi affetti:
UNIX(SGI/IRIX)

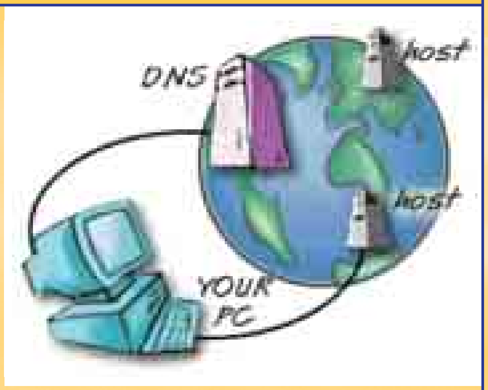
Versioni affette:
6.5 - 6.5.15

Soluzione:
Patch rilasciate e rilascio di IRIX 6.5.16. SGI raccomanda l'upgrade alla versione 6.5.16 quando disponibile.

DENIAL OF SERVICE CON DNS BIND V.9

CERT/CC ha emesso un alert riguardante una vulnerabilita' del DNS BIND v.9 (solo le versioni antecedenti la 9.2.1) di tipo 'denial of service'. Inviando un pacchetto DNS opportunamente costruito è infatti possibile determinare una condizione di errore nel server DNS e provocarne il suo shutdown.

Si consiglia di procedere rapidamente all'aggiornamento del BIND considerata l'importanza del corretto funzionamento di un servizio DNS.

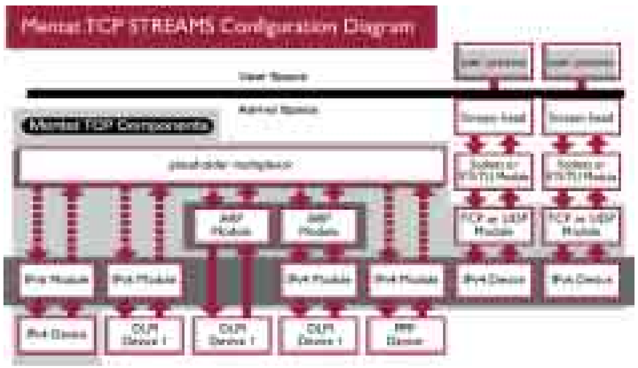


Maggiori informazioni possono essere reperite agli URL:
http://www.cert.org/advisories/CA-2002-15.html
http://www.isc.org

"COMPUTER: MACCHINA PROGETTATA PER VELOCIZZARE E AUTOMATIZZARE GLI ERRORI".

> Anonimo

QUANTUM SNAP 4100/160G: RISCHIO DoS



Il quantum snap server 4100/160G è affetto da una vulnerabilita' di tipo Denial of service e da un incorretta implementazione della gestione del TCP Sequence Number Risoluzione : politiche di firewalling tra l'appliance e la rete untrusted.

IPV6 PER WINDOWS XP



Ne parliamo abbondantemente all'interno di questo numero. Si tratta del protocollo di connessione IPv6 destinato a sostituire il "vecchio" IPv4. E' stato rilasciato da Microsoft un paper di installazione di IPV6 su Windows XP **http://www.microsoft.com/windowsxp/pro/techinfo/administration/ipv6/default.asp.**

DAMMI 5 $ CHE TI MIGLIORO I VOTI

Due giovani crackers Usa avevano ideato un bel sistema per far soldi: si collegavano al data base della Western High School di Davie, in Florida, e modificavano i voti negativi in voti positvi per soli 5 dollari. Ma hanno esagerato e li hanno beccati.

LINUX DAY IN ITALIA

Si terrà il 23 novembre il prossimo Linux Day in Italia, la manifestazione nata per promuovere Linux e il Software Libero.
La ILS, Italian Linux Society, invita tutti i Linux User Group (LUG) italiani e tutti quelli che utilizzano e intendono promuovere il software libero a stabilire, organizzare e pubblicizzare eventi in occasione del 23 novembre.
La filosofia è semplice: "l'eventuale utilizzo di software proprietario deve essere solamente occasionale, e non funzionale alla manifestazione.
Ciò significa che è eventualmente possibile tenere in considerazione anche software proprietario, ad esempio per questioni di interoperabilità, o in mancanza di un equivalente libero, o in risposta a richieste in proposito eccetera, purché sia chiaro che lo scopo della manifestazione non è la promozione di tale software".



I singoli eventi del Linux Day possono essere realizzati dagli interessati che dovranno però contare sulle proprie energie ed eventualmente su materiali e indicazioni provenienti da ILS. Invece l'accesso a tutti gli eventi dev'essere aperto a chiunque e non sarà dunque possibile per nessuno chiedere biglietti di ingresso a pagamento o altri oneri neppure per il materiale distribuito nel corso degli eventi.

HOT CUP!

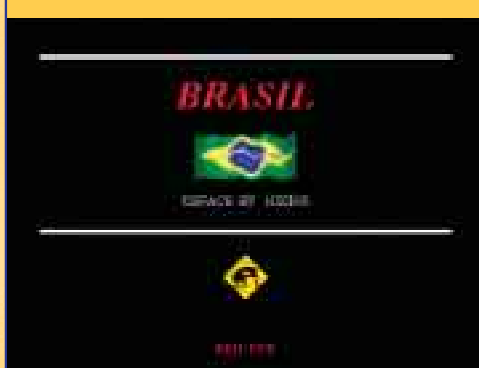
I CRACKER E I MONDIALI

Sempre in tema di mondiali di calcio sembra che i siti ad esso collegati siano presi di mira con un certo accanimento dai cracker. Il sito britannico www.fifa-wc-2002.co.uk, nato recentemente per rispondere alla fame di notizie e commenti dei navigatori inglesi è stato defacciato ad opera di un gruppo di cracker provenienti dal Brasile dove, oltre ai maestri del pallone, si sforna continuamente anche "fuoriclasse" del defacement.
Al posto della home page sono state inserite, manco a dirlo, imamgini del brasile di cui si auspica la vittoria finale.



INTERBUSINESS TIFA BRASILE

Il sito Interbusiness.it ha alzato bandiera, non bianca, ma verde/oro. Infatti chi ha operato il defacemet del sito ha lasciato come firma una bella bandiera brasiliana e si è firmato NIX$3R: che sia un tifoso della nazionale carioca e abbia fatto il gesto per propiziare la vittoria ai mondiali del Brasile? Ai posteri l'ardua sentenza, intanto forza Ronaldo!



LA CRITTOGRAFIA PER DIFENDERE LA PRIVACY

Camouflage: come

Avete una fitta corrispondenza via e-mail con una o più amanti? Trovate la cosa divertente, messaggio? Bene, potete tranquillamente smettere di preoccuparvi perché vi insegniamo



Crittografia: Sistema che consente di rendere maggiore la sicurezza di un file tramite codifica. Una volta che un file è stato crittografato, per poter essere letto deve essere decrittografato. Per cifrare file e documenti si possono usare programmi shareware liberamente scaricabili da internet.

L'e-mail è ormai uno dei mezzi di comunicazione più diffusi al mondo, e tutti la usiamo per i più disparati scopi. Non tutti sanno però che questo non è un modo molto sicuro di comunicare per molteplici motivi: basti pensare a sistemi di sicurezza come Echelon o ai numerosi passaggi di ogni nostra e-mail sui server di mezzo mondo. L'unico modo per evitare di lasciare sparse le nostre tracce per tutto il Net e per evitare che la moglie impicciona, sbirciando nella nostra mailbox, scopra le lettere della nostra amante è quello di dotarsi di un programma di cifratura dei messaggi.

Il programma di crittografia storico e dai più ancora utilizzato è PGP (Pretty Good Privacy, facilmente reperibile tramite un motore di ricerca) che si basa su un sistema ibrido simmetrico-asimmetrico nella gestione delle chiavi.

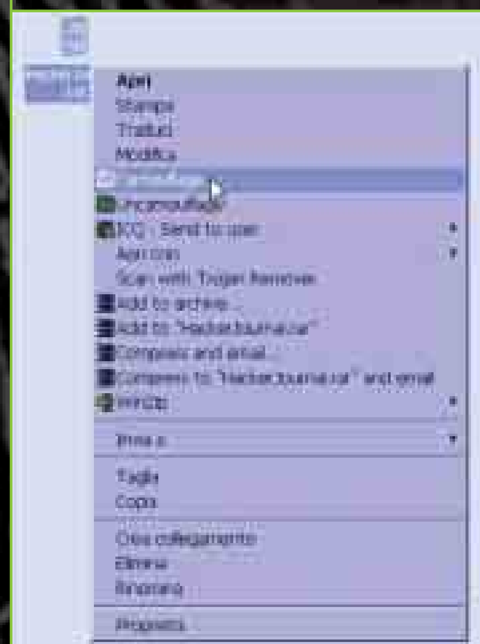
L'inconveniente di programmi di questo tipo, oltre alla loro relativa difficoltà di utilizzo, è quella di mostrare i messaggi palesemente crittografati insospettendo non poco la moglie o il capoufficio di turno che si trovano di fronte tali geroglifici.

È questo il motivo per cui in questo articolo rivolgeremo la nostra attenzione ad un altro programma, il Camouflage, che permette di mimetizzare qualunque tipo di file o testo all'interno di un altro file.

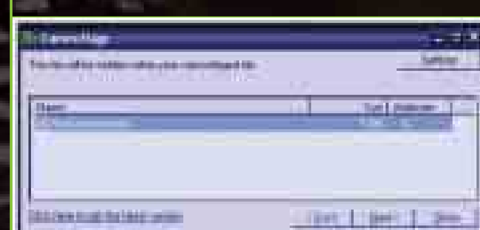
Chi penserebbe mai che nella foto raffigurante un cucciolo di cane si possa nascondere il messaggio della vostra amante o il progetto segreto su cui state lavorando durante le ore d'ufficio? Prima di tutto bisogna scaricare il programma, freeware, dal sito **camouflagesoftware.com**.

Dopo una rapida installazione, la prima cosa da fare è decidere su quale file nascondere il nostro testo.

Noi utilizzeremo un file grafico per nascondere un file di testo, ma è bene sapere che è possibile servirsi di qualunque file seguendo la medesima procedura. Una volta deciso il file da utilizzare, bisogna semplicemente cliccare con il tasto destro del nostro mouse sul file che abbiamo deciso di mimetizzare:



Ci troveremo ora di fronte a questa schermata:

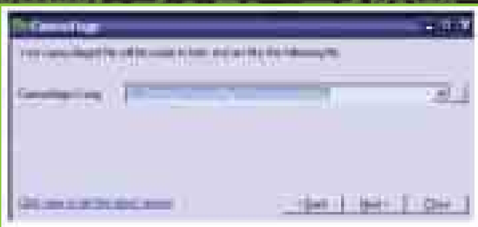


Selezionando il tasto Next si giungerà di fronte alla schermata dove inserire il percorso dell'immagine che abbiamo deciso di utilizzare come copertura (nel nostro caso la copertina di Hacker Journal):

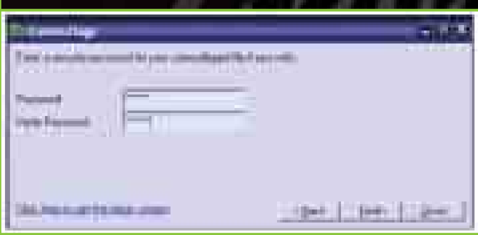
ti camuffo l'e-mail

appagante ma avete il sospetto che la vostra dolce metà possa intercettare qualche

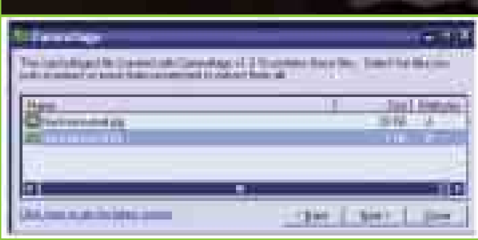
come cifrare i vostri messaggi con Camouflage: uno dei software di crittografia più diffusi.



Non ci resta che decidere il nome e la cartella di destinazione del nostro nuovo file e selezionare Next; successivamente avremo l'ultima schermata dove inserire la password (non obbligatoria) che ci permetterà l'accesso al contenuto nascosto del file:



Per poter leggere il contenuto celato nell'immagine basta cliccare con il tasto destro del mouse sul nuovo file, selezionare la voce "Uncamouflage" e inserire la password. Come per magia ecco riapparire i due file allo stato originale:



Un doppio click, all'interno di questa finestra, sul file di nostro interesse ci permetterà di leggere il contenuto top-secret del messaggio. Possiamo salvare i diversi file procedendo con il tasto Next .

ESEMPI DI CRITTOGRAFIA



Apparentemente è un dipinto, invece la sua trama grafica ne nasconde un'altra del tutto inaspettata...



... una visuale della Torre Eiffel vista dall'alto, miracoli della crittografia e dei software come Camouflage.



Potete mostrare a vostra moglie queste immagini che ritraggono paesaggi subacquei di rara bellezza...



... che celano un'altra bellezza tutt'altro che trascurabile: la vostra amante, abilmente mimetizzata.

Virus, se li conosci...

Volete difendervi da un virus? Magari un appendig dei file .com? Bene, allora dovete conoscere il "nemico". E per conoscerlo, occorre saperlo "costruire"...

Qui non si tratta di infettare tutta la rete sganciando virus come bombe in Afghanistan. Qui si tratta di capire bene che cosa sono i virus, come si costruiscono e come si procede, per poi potersi difendere quando si è attaccati. Infatti conoscere la tecnica di costruzione è essenziale per determinare le contromisure e le difese adeguate. Qui tratterò solo di un particolare tipo di virus, l'appending dei file COM. Per tutti quelli che non avessero letto la prima parte), ecco un breve riassunto di quanto detto finora riguardo l'infezione, in modo diretto, di un file COM:

Cercare un file di tipo COM sfruttando la funzione 4Eh dell'INT 21h (detta FINDFIRST).

Aprire il file in lettura (funzione 3Dh, sempre del DOS)

Cercare un marcatore o qualche altro accorgimento preso per segnalare un file come già infettato.

Se il file non risulta infetto, proseguire con l'infezione, oppure chiamare la funzione FINDNEXT (AH=4Fh del DOS) e ricominciare dal punto 2.

Questi pochi passi sono la parte iniziale di un virus. Non fanno nulla di speciale, se non cercare una vittima e "aprirla".

Come dovreste ricordare il nostro virus ha lo scopo di incollarsi alla fine del file, scrivere un'istruzione di salto (JMP) all'inizio del programma con cui far passare l'esecuzione al codice virale, e alla fine eseguire il file originale.

Per fare tutto ciò è indispensabile scrivere l'intero listato del virus ricordandosi che ogni riferimento a variabili, a puntatori di tipo FAR o altre istruzioni senza un OFFSET relativo, va fatto aggiungendo alla posizione in memoria dell'istruzione/variabile, la variazione dovuta alla diversa ubicazione che prende il virus nel file.





Come ricorderete avevamo lasciato l'infezione a metà e ci eravamo fermati a discutere del DTA. Avevo detto che serviva per ritrovare il nome del file da infettare. Ciò è vero in parte, poiché nel DTA troveremo moltissime informazioni sul file "vittima" ed alcune ci torneranno utili. Una delle prime cose da fare quando si scrive un virus è quella di non usare il DTA originale, ma di usarne una copia in memoria.

1) Individuare il file .com

Dopo aver trovato un file COM non ancora infettato dovremmo prenderci la briga di sprecare qualche riga di codice per salvare gli altri dati utili che si trovano nel DTA, come gli attributi del file, oppure la data e l'ora della sua creazione.

Ricordarsi di salvare queste informazioni è indispensabile (**o almeno lo era quando non c'era Windows**) per evitare di far scoprire subito l'infezione, infatti, una volta conclusa questa, tali dati dovranno essere rimessi a posto nel file. Altra cosa importante è quella di settare a zero gli attributi del file (dopo averli salvati): se per caso il file fosse Read Only, il virus non ci potrebbe scrivere dentro e non ci sarebbe infezione. Ecco quindi la necessità di togliere gli attributi del file per poi rimetterli a posto alla fine.

Appena trovato un file da infettare inizieremo col rendere il file "scrivibile" utilizzando la funzione 43h/01h del solito INT 21h che vuole in DS:DX il nome del file (ma per comodità potremmo usare un LEA DX,nome_file) e in CX l'attributo da dare al file ovvero 0. Dato che sotto Windows i virus ad azione diretta dei file COM sono praticamente inutili dovremmo immaginare di lavorare sotto DOS. In questo sistema operativo alcune sottigliezze come data e ora erano molto utili per celare un'infezione mentre sotto Windows lo sono relativamente. Quindi, per una questione di principio, insisteremo su questi dettagli.

2) Scrivere il file

Passiamo ora all'infezione e vediamo come scrivere nel file. Prima di sostituire i byte iniziali con l'istruzione di JMP al virus, ci si deve ricordare di salvare da parte quegli stessi byte che andranno sovrascritti. Il file deve essere aperto con l'istruzione 3Dh del DOS (**sintassi in tabella**), e dunque si procede con lo scrivere il codice esadecimale dell'istruzione JMP, ovvero E9, seguito dalla posizione del virus nel programma infetto. L'indirizzo di memoria del nostro virus non sarà sempre lo stesso, infatti dovremo calcolarlo in base alle dimensioni del file vittima.

La funzione per scrivere in un file è la 3Eh (trovate la sintassi delle funzioni in una tabella riassuntiva a fine pagina). Come output la funzione da in AX un handle (che spesso in italiano è erroneamente tradotto come "gestore") il quale servirà per identificare il file successivamente. Ma come avreste dovuto notare, alla funzione di scrittura, l'handle serve in BX. È quindi comodo usare l'istruzione XCHG AX,BX appena aperto il file, piuttosto che un MOV BX,AX che avrebbe reso il virus, anche se di pochissimo, più grande. Altra istruzione da usare al posto di MOV quando si deve far riferimento, ad esempio, a DI:DX, è un LEA (**Load Effective Address**).

Ricordate sempre, una dote che distingue un bravo virus writer dalle masse è saper ottimizzare al massimo il proprio "par-

goletto". Sarebbe opportuno tenere presente queste piccole accortezze che nei virus più "interessanti" risultano fare la differenza.

3) Inserire il JMP

Visto come si scrive nel file, vediamo come scrivere il nostro JMP in cima al programma. Si inizia col posizionare il puntatore all'interno del file all'inizio utilizzando la funzione 42h. Questa funzione chiede in AL il tipo di spostamento da fare (vedere tabella a fine articolo) in BX l'handle del file aperto, in CX:DX la posizione da prendere nel file e in DX:AX restituisce la posizione in cui si troverà il puntatore, dopo averla chiamata. Notate come questo possa anche essere un metodo alternativo per leggere le dimensioni del file: se mettiamo il puntatore alla fine del file, sapremo quanto misura controllando DX:AX. Dopo aver posizionato il puntatore non ci resta che scrivere il codice del JMP (**nella forma 0E9h**) seguita dalla posizione del parassita.

```
MOV AX,4200h; per muovere
il file
XOR CX,CX; azzera CX
XOR DX,DX ;azzera DX
INT 21h; infatti CX:DX =
00:00 ovvero
punta all'inizio del file

MOV AX,WORD PTR [BP+LUNGHEZ
ZA_FILE]; calcolo della
posizione del virus
SUB AX,3; toglie alle
dimensioni del file
dimensioni della parte
sovrascritta dal virus
MOV WORD PTR [BP+CODICE_JMP
+1], AX; mette da parte
il codice da scrivere
MOV AH,40h
MOV CX,3
LEA DX,CODICE_JMP
INT 21h
```

Questo pezzo di codice riassume quanto detto finora. In BX si trovi già l'handle del file ottenuto alla sua apertura, che sia già stato memorizzato in LUNGHEZZA_FILE la dimensione della vittima, e che esista una variabile CODICE_JMP contenete il valore 0E9h.

4) Creare il Virus

Dopo aver scritto il jump si deve scrivere il corpo del virus vero e proprio. Con la teoria fatta finora non dovrebbe essere difficile fare questa operazione. Si deve spostare il puntatore nel file dall'inizio alla fine. Ancora una volta ricorreremo alla funzione 42h ma con AL pari a 02h e di nuovo azzerando CX e DX.

Dopo esserci posizionati alla fine del file basterà copiare il corpo del virus e chiudere il file aperto. Per scrivere torneremo ad usare la 40h e come dati da scrivere ci basterà indicare la label di inizio del virus vero e proprio mentre il calcolo del valore da dare a CX lo faremo sottraendo alla fine del programma l'indirizzo di inizio.

```
Parte_1:
     JMP Parte_2
     Marcatore DB "M"
Parte_2:
. . . codice del virus . . .
Fine:
```

Rifacendoci allo schema di sopra faremo un LEA DX, [BP + Parte_2] per selezionare i dati da scrivere, mentre con un MOV CX, [Fine – Parte_2] troveremo il numero effettivo di byte da scrivere.

5) "Lavoro" ultimato

Fatto ciò il virus avrà infettato il file, non ci resta che chiuderlo chiamando la funzione 3Eh del DOS (col solito handle in BX e che una volta eseguita cancellerà il contenuto di AX), e restituire il controllo al programma originale.

Prima di continuare, un promemoria: onde evitare di creare un virus sovrascrivente (cioè che rovina il programma infettato) dovremmo ricordarci di salvare da parte il primo pezzo del programma dove sopra scriveremo il JMP al virus.

Questo si può fare anche quando si controlla un'eventuale marcatore leggendo i primi 4 byte del programma. Altra cosa da ricordare è quella di rimettere tutto a posto dopo aver infettato. Dovrete modificare di nuovo l'attributo del file per riportarlo di nuovo all'originale (di nuovo la funzione 4301h) e rimettere a posto la data e l'ora dell'ultima modifica.

Tutto ciò andrà fatto appena dopo aver chiuso il file vittima. C'è ancora una cosa da fare: prima di infettare sarebbe opportuno, appena il controllo passa al virus, salvare da parte i registri come DS e ES.

Un metodo potrebbe essere quello di pusharli per poi ripopparli prima di ridare terminare l'esecuzione del virus. L'esecuzione ne potremmo restituirla azzerando i vari registri di transito (AX, BX, CX, DX) e i registri puntatori DI e SI, il tutto tramite un comodo XOR, per poi chiudere il tutto con un RETF.

Si potrebbe anche far puntare i puntatori d'istruzione all'attuale posizione della prima parte del vecchio programma nel virus e poi saltare con un JMP alla stessa.

Detto ciò si conclude anche questa seconda parte che tratta della creazione di un semplice virus.

Con tutto quello detto finora probabilmente non riuscirete subito a farvi un virus e, in effetti, lo scopo prefissatoci non era tanto quello di dare codice "taglia/incolla" per farsi rudimentali "killer" ma piuttosto la possibilità di sfamare la curiosità di chi sui virus vorrebbe sapere un po' di più.

Se vorrete davvero diventare virus coder il mio consiglio è quello di studiarsi bene l'assembler (e anche il C), e di fare tante prove senza mai perdersi d'animo di fronte ai primi fallimenti.

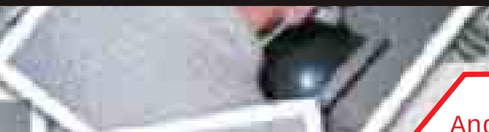
Se mi sarà concesso altro spazio nei prossimi numeri cercherò di trattare della criptazione e del polimorfismo oppure dei virus TSR che per quanto obsoleti hanno rappresentato un vero e proprio capitolo nel mondo dei virus.

[MiMMuZ]

6) Riassunto funzioni

INT FUNZIONE Descrizione
Chiude un file aperto. In BX va l'handle del file e AX viene cancellato al termine dell'operazione.
Scrive in un file aperto. In BX l'handle, in CX il numero di byte da scrivere e in DI: DX i dati da scrivere.
Sposta il puntatore in un file. In AL va il metodo (00h=da inizio file,01h=dalla posizione corrente, 02h=da fine file).
In BX va il gestore, in CX: DX lo spostamento desiderato, in DX: AX restituisce la nuova posizione.
Cambia gli attributi di un file. In DS: DX chiede il nome del file e in CX l'attributo da dare al file.

Virus: sapere programmare un virus è utile sia per difendersi, sia per risolvere problemi di program-mazione in senso lato.
JMP: E'un'istruzione di salto all'inizio del programma con cui far passare l'esecuzione al codice virale, ed eseguire il file originale






Andrei, professione… pirata!
Nome: xxxxxx
Età: 24 anni
Nazionalità: ucraino
Capelli: biondi
Occhi: blu
Professione: pirata

Il pirata ucraino

Dopo aver girato nella scena russa per un paio d'anni dove si divertiva nel penetrare (o almeno ci provava) nei sistemi informatici americani e tedeschi, Andrei si è ritrovato introdotto nell'ambito crackage "professionale" grazie ai suoi amici della scena underground. Il suo scopo: craccare i programmi e i giochi per metterli in vendita in versione piratata.

Cosa ti motiva nel hacking/craking?

Il fatto di poter guadagnare un centinaio di dollari. Perché molto spesso abbiamo bisogno solamente di un editore esadecimale e di qualche software che abbiamo sviluppato in C che ci permette di confrontare il code source per poter qualche ora defacciare qualsiasi programma nell'85% dei casi!

In concreto come funziona?

Il tutto varia enormemente in funzione degli editori di programmi. Riusciamo ad avere il più delle volte le versioni americane appena uscite e ne facciamo immediatamente una copia modificando il codice, e meno spesso, sviluppando una patch correttiva, da lanciarsi dopo l'installazione del programma o del gioco. Ultima possibilità piazzare un numero di licenza con la versione che noi distribuiamo.

Non avete dei problemi con la polizia?

Diciamo che bisogna saper salvare capra e cavoli. Cercare di dissuadere la polizia magari convincendola attraverso un generoso donatore per le "opere di carità" della polizia, se capite ciò che voglio dire! Ma su questo ultimo punto, noi non siamo chiamati a rispondere, è il nostro boss.

Vuoi dire che lavori per qualcun altro?

Sì, sicuramente qui non potete fare nulla a un certo livello senza avere delle basi ferree. Al mio livello, non rappresento nulla e non cerco d'altronde di tirare avanti da solo, è troppo rischioso.

Alludi alla mafia?

Non andiamo oltre! Si tratta di gruppi d'interesse comuni che non vogliono per forza spartirsi la torta, cosa che posso capire.

E perché non andare a lavorare in una azienda di informatica classica, per esempio all'ovest?

Non ho voglia di lavorare dieci ore al giorno per 250 dollari (225 euro) quando guadagno più di 800 dollari attualmente per qualche ora alla settimana! Per quanto riguarda andare ad ovest, bof, ho tutto di cui ho bisogno qui!

In quanti lavorate e come?

Siamo una piccola squadra di quattro persone, più una persona esterna che lavora da freelance a seconda delle nostre necessità: uno sviluppatore per software e la programmazione delle patches, due programmatori/crackers adibiti alla protezione, un designer per le sovracoperte e la fabbricazione dei cd che servono per la duplicazione, eventualmente, ed è sempre più frequente uno sviluppatore mediale che sviluppa l'interfaccia di presentazione dei cd pirata (i discendenti dei demomakers che creavano le demo allegate con i softwares pirati).

Come vedete il vostro futuro? E siete fiduciosi?

Sapete, il futuro si limita al mese che viene. Io guadagno bene la mia vita, non rischio più di tanto e vedrò a seguire quando ciò si presenterà.

Nessun cd dell'Europa dell'est arriva da noi, quando questo potrebbe rappresentare molto denaro, perché?

Non conoscono i segreti dei boss, so che è un qualcosa che interessa, ma per ora preferiscono star tranquilli.

CLONARE I CELLULARI È FACILE?

LE VIE DELLA CLONAZIONE SONO INFINITE...



Se pensate che clonare un cellulare sia impossibile, basta girare un po' nella rete per cambiare idea...

Sulla clonazione dei telefonini e sull'intercettazione dei messaggi telefonici sono disponibili una serie di divertenti leggende metropolitane e scherzi assortiti. Girando nei numerosi forum in internet può capitare anche di leggere che per ricaricare una carta telefonica a sbafo, basta cuocerla un po' nel microonde. Sconsigliamo vivamente la pratica perché si tratta sicuramente uno scherzo messo in giro da qualche burlone, anche se non dubitiamo che vi siano casi di SIM card "al cartoccio".

>> Crittografia a 128 bit

Nella realtà la protezione dei GSM (Global System for Mobile Communications), e in particolare delle comunicazioni, deriva dall'adozione di un sistema di trasmissione di dati crittografato. In pratica si tratta di una specie di alfabeto personalizzato che consente di inviare messaggi, nel corso della comunicazione, privi di alcun significato.

Facciamo un esempio: poniamo di volere comunicare la parola Milano, se come sistema di crittografia decidiamo di sostituire ciascuna lettera della frase con quella immediatamente successiva, la parola inviata sarà Nlmbop. Assolutamente priva di significato. Non per l'utente che la riceve perché questa parola crittografata viene codificata da un algoritmo di cifratura contenuto proprio nella SIM (la carta che attiva il cellulare) che, nel caso in esempio, avrebbe un valore 2. Per forzare una crittografia di questo tipo e intercettare i messaggi basterebbe forzare tutti gli algoritmi da 1 a 20, tante sono infatti le lettere dell'alfabeto, fino a trovare la chiave giusta.

Ma evidentemente il sistema di protezione di un GSM è ben più complesso. Si basa infatti su un algoritmo di codifica contenuto nella SIM che viene chiamato COMP128.

Tale algoritmo lavora su un messaggio crittografato che può essere tradotto solo da una SIM a128 bit (chiavi) e prevede oltre 150.000 possibili combinazioni. Se qualcuno volesse attaccarlo via etere dovrebbe stare collegato con la SIM card almeno otto ore consecutive. Mentre avendo tra le mani la Sim basterebbero pochi secondi per forzare il codice e clonare la scheda.

>> L'attacco dividente

Proprio partendo da questo ultimo postulato, il gruppo di ricerca dell'IBM ha individuato un nuovo sistema di attacco (dividente) alle schede che consente di reperire le informazioni chiave segrete dalle SIM controllando le lato-scanalature, come assorbimento di corrente di energia e le emanazioni elettromagnetiche (EM). L'attacco può ottenere le informazioni chiave in pochissimi minuti. Come afferma Charles Palmer, gestore del gruppo di reparto di sicurezza, della segretezza e del cryptography a ricerca dell'IBM. "I telefoni di GSM stanno aumentando e sempre più spesso prevedono toolkits di applicazione di SIM che permettono operazioni quali: transazioni bancarie e servizi aggiuntivi. In tutte queste situazioni, le informazioni di identificazione sono salvate sulla scheda di SIM. Se questi toolkits non sono concepiti con attenzione per proteggerli dagli attacchi, compresi gli attacchi "dividenti", allora per un hacker è possibile duplicare le informazioni sulla scheda un modo molto semplice."

La ricerca dell'IBM ha sviluppato una nuova tecnica per proteggere i funzionamenti di consultazione di tabella, che si verificano, ad esempio, quando la SIM viene usata per transazioni bancarie, dagli attacchi laterali della scanalatura. Quando si imposta un'operazione sulla SIM sostanzialmente viene controllata una tabella nella memoria del calcolatore per richiamare un valore memorizzato in una posizione particolare. I ricercatori hanno progettato una tecnica che prevede una sequenza delle consultazioni di tabella con posizioni completamente casuali, che non forniscono informazioni rilevanti. Questo rimontaggio è realizzato usando una piccola tabella generata casualmente, una specie di "specchietto per le allodole" tecnologico. Le informazioni laterali della scanalatura sostanzialmente sono camuffate e diventano inutili ad un hacker. Poiché la tecnica proposta usa poca RAM per la tabella dipendente, può essere applicata facilmente per proteggere una grande varietà di dispositivi di memoria, comprese le SIM.

I possessori di GSM possono comunque proteggersi con metodi meno tecnologici ma altrettanto efficaci: come evitare di prestare il telefonino a sconosciuti e di lasciarlo incustodito.

?

Gprs General Packet Radio System: Standard per la trasmissione dati nella rete telefonia cellulare attraverso la commutazione di pacchetto,sopporta inoltre la commutazione di circuito (GSM),che gli SMS. La massima velocità e di 115,2 Kbps .utilizzando contemporaneamente tutti gli otto timeslot disponibili, contro i 9,6 Kbps del GSMr.

?

Dual Band: Cellulari GSM compatibili con entrambi le tecnologie digitali a 900Mhz che 1800 Mhz

IPv6: un nuovo pro

IPv6 è un protocollo di connessione destinato a mandare in pensione il

Cos'é L' IPv6? IPv6 sta per "Internet Protocol version 6" ed è il protocollo designato a rimpiazzare l'attuale protocollo su cui si basa internet, detto IPv4. La maggior parte (In pratica il 100%) degli utenti Internet usa IPv4, un protocollo ormai vecchio di 20 anni con molte falle di sicurezza, appunto da far pensare alla progettazione di un nuovo protocollo. Secondo e ben più importante motivo della nascita dell'IPv6 è la "mancanza" di indirizzi IPv4 assegnabili, che stanno ormai per terminare, ma dei quali hanno bisogno le nuove macchine connesse ad Internet.

L'IPv6 attualmente è in co-esistenza con IPv4, appoggiandosi ad una rete IPv6-Over-IPv4 chiamata 6bone, la quale appoggia a sua volta sulla attuale rete Internet IPv4, tramite un sistema di tunneling dati IPv6 inseriti in normali pacchetti IPv4. Le aspettative sono che, fra qualche anno, IPv6 Rimpiazzerà completamente IPv4.

>> Da decimale a esadecimale

La differenza sostanziale fra IPv6 e IPv4 è nella struttura degli indirizzi, che **nella vecchia versione dell'Internet Protocol è in base dieci (es: 62.98.231.67), mentre nella nuova versione è in base 16 (esadecimale)**. Un esempio di IPv6 può essere: 2001:6b8:0:400::70c (corrisponde al mio IPv6 attuale :)).

Vediamo meglio la sua struttura: Il nuovo IP è formato da 8 blocchi di 16 bit l'uno. Guardando l'esempio precedente noterete che i blocchi non sono 8 ma 6, in effetti sono 8 ma due blocchi sono racchiusi tra " :: " perché sono tutti zeri. Nella forma completa quindi sarebbe stato: **2001:06b8:0000:0000:0400:0000:0000:070c**.

Un'altra forma di scrittura dell'ipv6 è la **Nibble**. Questa forma è usata per la zona inversa dei DNS (Domain name Server).



> **DNS**: Domain Name System.
> È il sistema che permette di far corrispondere un dato dominio al relativo indirizzo ip, in modo che digitando il nome del dominio di un sito, l'utente venga connesso al computer che effettivamente ospita quel sito.

Questa forma prevede che l'IP venga scritto al contrario, cifra per cifra, senza contrazioni e che ogni carattere venga separato da un punto. Facciamo un esempio: se l'ip è: 2001:6b8:0:400::70c, nella forma nibble sarà **c.0.7.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.0.0.8.b.6.0.1.0.0.2.ip6.int**.

Si è un po' lunghetta... Sono esattamente 32 caratteri + i punti + ip6.int. Quindi quando dovrete scriverlo in questa forma ricordatevi che ci devono essere 32 caratteri.

Altra novità è che la netmask che nella v4 era usata per individuare nodi e reti scompare e viene sostituita dal prefix. Il prefix è quella scritta che segue l'IP ovvero /16 /64 /127 .

A cosa serve? A dirvi quanti IP vi sono stati dati, o meglio il numero di bit fissi.

Per esempio se vi viene data una /128 voi non potete modificare nessuna cifra xche tutte le cifre sono fisse (128 bit).

Se vi danno una /120 vuol dire che avete a disposizione 256 IP. Come ho ottenuto questo numero? Bene ho sottratto al numero massimo di bit il numero di bit fissi quindi 128-120=8 e questo mi dice che 2 elevato all'ottava è il numero di IP che posso usare. È da considerare che gli indirizzi IPv6 assegnati dai Tunnel Broker (ovvero dei provider che offrono servizi di tunneling IPv6-over-IPv4 gratis) sono statici, pertanto si può usufruire della comodità di un IP statico, risolvibile in un nome di dominio via DNS senza dover essere aggiornato ad ogni cambio di IP. I piu` recenti sistemi operativi (Sistemi Win a partire da Win2k(SP1)) Sono dotati di supporto del tunneling IPv6-Over-IPv4 integrato. In alcune distribuzioni Linux per installare il protocollo IPv6 è necessaria una ricompilazione del kernel (per i kernel monolitici) mentre per altre, del semplice e indolore caricamento del modulo relativo a IPv6 (modprobe ipv6). Per funzionare, un tunnel IPv6 ha bisogno di essere configurato da 2 lati: Lato server (il Tunnel Broker) e Lato client (il nostro PC). Il lato server viene configurato autonomamente dal tb(tunnel broker), mentre per la configurazione del lato client tocca a noi =).

Per attivare un tunnel di dati IPv6-Over-IPv4, ovviamente bisogna essere iscritti ad un tunnel broker, di cui parlavo in precedenza.

I tunnel broker Italiani più famosi al momento sono: Edisontel, NGnet(telecom Italia), 6b0ne.org e 6bone.ws . Ogni tb ha delle procedure di autenticazione ed aggiornamento IPv4 differenti, ma non di molto. In ogni caso, sulle homepage dei tunnel broker sono presenti How-To e FAQ abbastanza esaurienti. Dopo essersi iscritti ad un tb, si dovrebbe ricevere una email con i dati del proprio tunnel, che sono: login e password.

Proprio Indirizzo IPv6 (e/o la propria Subnet, se ve ne è stata assegnata una)

Endpoint IPv4 (**ovvero l'ip del tunnel broker**)

Endpoint IPv6 (**l'IPv6 del tunnel broker, non sempre necessario**)

E' da considerare il fatto che il tunnel broker, per consentire il transito di dati IPv6 su pacchetti IPv4 e per configurare il "lato

tocollo per Internet

vecchio IPv4, che peraltro potrà ottenere l'adeguamento della "minima"

server" prima accennato deve conoscere il nostro indirizzo IPv4, il quale (essendo nella maggior parte dei casi dinamico, salvo linee a banda larga tipo xDSL, etc) deve essere aggiornato a mano sul sito web del proprio tunnel broker, oppure con degli script appositi (script bash per Linux, script Perl per Win), che tramite richieste HTTP, evitano di inserire a mano login, password e Indirizzo IPv4.

Per verificare se c'è bisogno o meno della ricompilazione del kernel di Linux, digitate (da root):

```
[root@localhost/root]#modprobe ipv6
```

Fatto questo, digitate:

```
[root@localhost/root]#ifconfig
```

Se siete fortunati, e la vostra distro supporta IPv6 nativamente, l'output di "ifconfig" sarà qualcosa simile a:

```
lo Link encap: Local Loopback
inet addr: 127.0.0.1
Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host->
La riga che ci interessa, se
avete questo iniziate a saltare
di gioia per la casa=)
UP LOOPBACK RUNNING
MTU:16436
Metric:1
RX packets:20 errors: 0 dropped:
0 over
runs:0 frame: 0
TX packets: 20 errors: 0 dropped:
0 overruns: 0 carrier:0
collisions: 0 txqueuelen: 0
RX bytes: 1400 (1.3 Kb) TX
bytes:1400 (1.3 Kb)
```

In questo esempio viene elencata solo l'interfaccia lo e nessuna interfaccia ppp perché il comando è stato eseguito offline =)

```
[root@localhost /root]#
```

Dopo aver fatto ciò, per sicurezza pinghiamo il corrispondente di localhost (127.0.0.1) in ipv6, ovvero ::1

```
[root@localhost/root]# ping6 ::1
```

Se tutto e' ok , osserverete un output del genere (per interrompere i ping, CTRL-C)

```
PING ::1(::1) from ::1 : 56
data bytes
64 bytes from ::1: icmp_seq=0
 hops=64 time=55 usec
64 bytes from ::1: icmp_seq=1
hops=64 time=45 usec
64 bytes from ::1: icmp_seq=2
hops=64 time=44 usec
64 bytes from ::1: icmp_seq=3
hops=64 time=46 usec
64 bytes from ::1: icmp_seq=4
hops=64 time=45 usec
64 bytes from ::1: icmp_seq=5
hops=64 time=47 usec
64 bytes from ::1: icmp_seq=6
hops=64 time=42 usec
--- ::1 ping statistics ---
7 packets transmitted, 7 packets
received, 0% packet loss
round-tripmin/avg/max/mdev=
0.042/0.046/0.055/0.006 ms
[root@localhost /root]#
```

Se invece non avete fatto i salti di gioia perché la vostra distribuzione Linux non supporta IPv6 nativamente, non correte a prendere la vostra rivoltella nel cassetto; bensì leggete sotto tenetevi forte, ci aspetta un avventuroso viaggio nella ricompilazione del kernel di linux!!!

Vi ricordo che per ricompilare il kernel, dovete avere i suoi sorgenti in /usr/src/linux se non li avete procurateveli dai cd della vostra distro oppure scaricateli da www.kernel.org. Ecco i passi necessari per attivare il protocollo IPv6 durante la ricompilazione del kernel:

```
cd /usr/src/linux

make menuconfig
```

```
Per Kernel 2.2.x selezionate:
Code maturity level options
[*] Prompt for development
and/or
incomplete code/drivers
Networking Options
[*] Kernel/User netlink socket
[*] Netlink device emulation
[*] The IPv6 protocol (EXPERIMENTAL)
[*] IPv6: enable EUI-64 token format
[*] IPv6: disable provider based
addresses

Per Kernel 2.4.x selezionate:
Code maturity level options
[*] Prompt for development
and/or
incomplete code/drivers
Networking Options
[*] Kernel/User netlink socket
[*] Routing messages
[*] The IPv6 protocol (EXPERIMENTAL)
```

Uscite e digitate al prompt:

```
make dep

make clean

make bzImage

cd /usr/src/linux/arch/i386/boot
```

Ora che abbiamo in nostro nuovo kernel con l'ipv6 abilitato dobbiamo farlo partire all'avvio quindi facciamo:

```
cp bzImage /boot/bzImage6
```

E' importante che non sovrascriviate il vecchio bzImage, quindi durante la copia cambiategli nome, io per esempio ho messo bzImage6. Ora andiamo sul file di configurazione del lilo per dirgli che all'avvio vogliamo scegliere se far partire linux col vecchio o col nuovo kernel, quindi:

cd /etc Editiamo il file di configurazione di lilo:
pico lilo.conf (oppure lo editate con un editor grafico). Alla fine del file aggiungiamo:

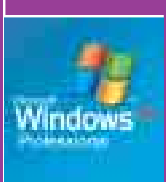
```
image=/boot/bzImage6
label=IPv6read-only
root=/dev/hda2
```

Stiamo bene attenti a mettere un label diverso da quello delle righe precedenti, io per esempio ho messo IPv6. Salviamo il file e per vedere se tutto a posto scriviamo: lilo e come risposta dovremmo avere:

```
linux* IPv6
```

Se è così ora non rimane altro che resettare la macchina e all'avvio scegliere il nuovo kernel. A questo punto se digitate ifconfig dovrebbe apparire fra le varie interfacce quel famoso INET6 di cui ho parlato prima. Per maggiore sicurezza, provate a pingarlo come detto prima " ping6 ::1 ". Ecco come fare Per installare IPv6 Da Win2k:

>> Installiamo IPv6 da Win2000/XP



Assicurarsi che il proprio Windows 2000 sia aggiornato con il Service Pack 1 o 2, altrimenti lo si dovrà aggiornare prima di procedere. Se il proprio Windows 2000 è aggiornato al Service Pack 1 scaricare lo stack per SP1, altrimenti se è aggiornato al Service Pack 2 scaricare lo stack per SP2(semplice). Una volta scaricato lo stack IPv6 adatto, installalo seguendo le istruzioni a video. (per SP2 è sufficiente eseguire hotfix dalla cartella setup). A questo punto seguire i seguenti passi: (se disponi di una scheda ethernet installata salta direttamente al punto 7)

1. Start -> Impostazioni -> Pannello di controllo e seleziona Installazione nuovo hardware

2. Selezionare Aggiungi/risolvi problemi e quindi cliccare su Avanti

3. Dall'elenco mostrato selezionare Aggiungi nuova periferica e cliccare su Avanti

4. Adesso selezionare No, l'hardware sarà selezionato da un elenco e cliccare nuovamente su Avanti

5. Selezionare Scheda di rete, quindi cliccare su Avanti

6. Nella colonna "Produttori" selezionare Microsoft e nella colonna "Scheda di rete" selezionare Scheda Microsoft Loopback poi cliccare su Avanti

7. Cliccare su Start -> Impostazioni -> Rete e connessioni remote, premere il tasto destro su Connessione alla rete locale e selezionare "Proprietà"

8. Dovrebbe aprirsi una nuova finestra dalla quale cliccare su "Installa"

9. Adesso selezionare Protocollo e poi cliccare su "Aggiungi"

10. Selezionare "Microsoft IPv6 Protocol": hai finito.

Nel caso avessimo a che fare con l'ultimo sistema (dis)operativo di casa Microsoft, le cose diventano molto piu' facili: per installare il protocollo IPv6, infatti...

```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\VIP3R>ipv6 install

Installazione in corso...Operazione riuscita.
```

...Ed ecco fatto. Al massimo e' richiesto un riavvio della macchina.

Ora vediamo come configurare la propria macchina per permettere il tunneling IPv6-Over-IPv4.

Configuriamo Il lato Client (Win2k/XP)

Questa fase è uniforme, non ci sono differenze fra i 2 sistemi operativi Microsoft che supportano IPv6. 2 comandi: uno per connettersi all'Endpoint IPv4, un altro per "alzare" il proprio IPv6 assegnatoci dal tunnel broker.

Vediamo il primo...

```
ipv6 rtu ::/0 2/::PROPRIO.ENDPOINT.IPv4 pub
----> ipv6 rtu ::/0 2/::xxx.xxx.xxx.xxx pub
```

Ed ecco il secondo...

```
ipv6 adu 2/PROPRIO:IPv6 ---->ipv6adu2/xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
```

Configuriamo Il lato Client (Linux)

Per Linux, i comandi variano da distribuzione a distribuzione. Essenzialmente sono 3:

1. Per alzare l'interfaccia sit0, ovvero un interfaccia di rete IPv6-Over-IPv4 digitiamo:

```
[root@localhost viper]#ifconfig sit0 up
```

2. Ci assegniamo il nostro IPv6:

```
[root@localhost viper]# ifconfig sit0 inet6 add il:nostro:ipv6
```

3. Ci connettiamo all'endpoint IPv4 con:

```
[root@localhost viper]# route -A inet6 add ::/0 gw ::endpoint.ipv4 sit0
```

Et voilà, les jeux sont faits!

by Viper

LINKS

Comunque, per ulteriori informazioni sul protocollo IPv6, su come installarlo su altri sistemi operativi (es.: **freebsd o MacOS**) e sulla struttura del networking vi rimando ai seguenti URL:

Tunnel Broker Edisontel
http://www.6bone.it
AltroTunnel Broker
http://www.6b0ne.org
Sito in italiano su IPv6
http://www.ipv6mania.net
Altro sito Italiano su IPv6
http://www.xunil.it
Tunnel Broker di Telecom Italia Net
http://tb.ngnet.it
Il miglior sito di IPv6, in inglese
http://www.hs247.com
Hurricane Electric, Tunnel Broker Americano
http://ipv6tb.he.net
Ennesimo Tunnel broker Europeo
http://www.freenet6.net

DOVE RECUPERARE LE UOVA DI PASQUA IN RETE

UOVA DI PASQUHACK

Volete vedere Bill Gates nudo? No, perché non lo potete vedere neanche vestito? Beh, peccato perché approfittando delle Easter Eggs che affollano i programmi commerciali potreste vivere questa indimenticabile esperienza...

Se si parla di Uova di Pasqua viene abbastanza immediato pensare a quelle di cioccolato con annesse sorpresine. In realtà esistono altre uova di pasqua che sono di natura esclusivamente informatica e che, con quelle di pasticceria, hanno in comune solo la sorpresina che nascondono. Con questo curioso nomignolo infatti si indicano i segreti nascosti nei programmi di grande diffusione, si pensi, ad esempio, a Word o Excel e che possono essere attivati solo utilizzando alcuni tasti o scrivendo alcuni codici particolari. Le uova di pasqua sono spesso piccoli scherzi dei programmatori, oppure, come nel caso delle cheat dei videogames, scorciatoie che i programamtori inseriscono per arrivare ad un certo punto del programam e togliere dei bug. Esistono diversi siti che fanno della propria missione proprio la raccolta di questi codici segreti. Uno dei più famosi è www.eggheaven2000.com che si prende la briga di dividere tutti i trucchi per piattaforma: PC, Apple, Linux. Tra i più divertenti rintracciati al suo interno segnaliamo il Pinball che si può attivare aprendo un nuovo documento di Word (per PC). Ma gli esempi non mancano...



Simulatore di volo per Excel:

1. Aprite un nuovo worksheet, e premete F5.
2. Scrivete X97:L97, e date Invio.
3. Premete il Tab. Premendo Ctrl-Shift, fate click sul bottone Chart Wizard nella toolbar.
4.Usate il mouse per volare: il tasto destro vi fa andare avanti, quello di sinistra vi fa capovolgere.

Volete qualcosa di più spettacolare? Avete l'esigenza di stupire amici e conoscenti a tutti i costi?
Non c'è problema, il sito segnala un trucchetto davvero d'effetto: utilizzando una serie di tasti con Wine Guide è possibile vedere Bill Gates nudo e chissà se il boss della Microsoft avrà gradito questo scherzetto da parte dei suoi dipendenti.
Se qualcuno poi conosce un trucchetto nuovo lo può segnalare a Eggsheaven accedendo nella apposita sezione: sono proprio queste segnalazioni a determinare il successo e la crescita del sito.
In Italia trova spazio l'indirizzo www.eastereggs.it che propone una guida alle "uova di pasqua" più gustose. Molte sono tradotte in italiano da siti similari, ma si trovano anche diverse chicche.
Una, in Excel, permette di attivare un simulatore di volo nascosto pilotabile, poi, con l'ausilio del mouse.
Funziona solo con Excel 97 e anche qui bisogna aprire una piccola parentesi: non tutti i trucchi funzionano sempre, anche se si possiede la versione indicata, come spesso avviene anche per i trucchi per i videogiochi a volte il funzionamento è limitato ad una certa serie commercializzata in un determinato periodo e non in quelle successive. Ci vuole un po' di pazienza e di fortuna.

SCHEDE

Se volete avere sottomano tutte le risorse per scovare i trucchi segreti dei programmi l'indirizzo che fa per voi è http://www2.webmagic.com/eastereggs.com. Si tratta di un portale degli "scherzetti" che cataloga tutti i siti rilevanti in materia e propone i link diretti. Nel sito sono suggeriti anche libri che si occupano dell'argomento, perché in fondo gli scherzi sono una cosa maledettamente seria. Sono quasi tutti acquistabili on-line su Amazon.
I possessori di Macintosh non devono disperare: non tutte le "uova" sono contenute in programmi Windows compatibili, all'indirizzo http://humanum.arts.cuhk.edu.hk/~cmc/mirror/chngai/easter-eggs (Mac Os Easter Eggs) sono riportati tutti i trucchi per Apple, suddivisi per categoria.
Un ultimo sito che dà dritte preziose in tema di scherzetti è www.eeggs.com/tree: molti i trucchetti suddivisi tra applicazioni, giochi, hardware e sistemi operativi con la possibilità di impostare una ricerca mirata.

TUTTI I PROTOCOLLI DI CONNESSIONE ALLA RETE



Una questione di “protocollo”

Il collegamento a Internet, per quanto banale, si basa su una serie di connessioni complesse... Vediamo quali!

Quando si parla di reti di computer spesso le persone poco esperte seppure appassionate storcono il naso dicendo: "Troppo difficile bisogna essere degli scienziati per capire quelle robe lì!" Falso nella maniera più assoluta specialmente grazie all'enorme progresso tecnologico (e alle guide come questa :-P) che ha investito l'ambiente informatico negli ultimi anni. Grazie ad esso infatti tutte le faccende che prima sembravano un po' più ostiche ora risultano parecchio semplici anche per gli utenti meno esperti. Certo è impensabile non parlare della teoria che sta dietro le reti informatiche anche perchè si tratta degli argomenti un po' più complessi dell'informatica quindi, Il mio scopo è di informarvi il più possibile sulle novità e sui cambiamenti delle reti informatiche di tutti i tipi... quindi parleremo di reti e protocolli informatici che hanno fatto storia e che tuttora sono in grande sviluppo....

Protocollo IPv6 (vedi articolo esteso)
Protocollo TCP
Protocollo netbios/netbeui
Protocollo IPX/SPX
Protocollo AppleTalk
La Rete Token-Ring
La Rete Ethernet
Le tipologie di rete

>> Protocollo Tcp

In realtà definire il TCP/IP un protocollo non è molto corretto. Sarebbe meglio dire che è un insieme di protocolli che comprendono TCP, IP, UDP ed altri protocolli. Cerchiamo comunque di dare un'idea di che cosa è il TCP/IP. Per trasmettere dei dati tra due calcolatori bisogna avere la possibilità di identificare univocamente i due calcolatori e questo è possibile mediante un indirizzo, l'indirizzo IP, che ovviamente deve essere unico per ogni calcolatore. Vedo di dare una breve idea del meccanismo di funzionamento del TCP/IP. In realtà sono due distinti protocolli il TCP e l'IP. Il protocollo IP (Internet Protocol) è il protocollo che consente la trasmissione di dati tra due calcolatori identificati univocamente mediante il loro indirizzo IP. La trasmissione dei dati mediante il protocollo IP segue uno schema semplicissimo, i dati da trasmettere sono suddivisi in pacchetti di una certa dimensione, ad ogni pacchetto è associato l'indirizzo del mittente e l'indirizzo del destinatario quindi il pacchetto viene inviato.

Il protocollo IP non prevede alcun controllo sui dati trasmessi, non verifica che tutto ciò che si è trasmesso arrivi a destinazione e non verifica nemmeno che i pacchetti giungano a destinazione nell'ordine corretto con cui sono stati inviati. In realtà può capitare che un pacchetto trasmesso dopo arrivi prima di un altro a destinazione perché nella rete IP ha preso una strada più corta. Il protocollo TCP lavora in coppia con l'IP, questo protocollo si preoccupa della correttezza delle trasmissioni, verifica che tutto ciò che è stato inviato sia arrivato effettivamente a destinazione ed eventualmente chiede la ritrasmissione dei dati andati persi. Verifica inoltre che la sequenza di ricezione sia la stessa della trasmissione, in caso contrario prevede un meccanismo per risistemare la corretta sequenza dell'informazione. Il TCP si basa sul protocollo IP per l'invio fisico dei dati.

>> Protocollo netBios/NetBeui

NetBios (NetWork Basic Input/OutPut System) è in sostanza un insieme di regole che dettano in che modo le applicazioni debbano accedere alla rete, sviluppato congiuntamente da IBM e da Microsoft negli anni '80, implementando nativamente nei sistemi operativi Microsoft e dal funzionamento relativamente semplice. Ogni computer viene identificato in rete da un nome specificato al momento dell'installazione del sistema operativo valido come indirizzo del destinatario. Quando dei dati vengono attraverso un pacchetto NetBIOS, ogni computer connesso alla rete stessa ne riceve una copia che viene scartata se non è l'indirizzo del destinatario. Questo sistema pur essendo semplice degrada le prestazioni della rete in quanto il traffico gestito in questo modo sarebbe costituito maggiormente da pacchetti inutili e quindi destinati ad essere scartati. Inoltre non permettono di interfacciare direttamente diverse reti tra loro e non possono accedere all'esterno, di conseguenza verso una rete come internet rimane limitato alle piccole reti chiuse dove cmq è in grado di ottenere prestazioni di tutto rispetto se il numero dei computer è limitato. Altri vantaggi consistono nella quasi completa assenza di procedure di configurazione, a esclusione dell'inserimento del nome al momento dell'installazione e nel ridottissimo spazio di occupazione in memoria che il software di gestione richiede.

>> Protocollo Ipx/Spx

IPX/SPX (Internetwork Packet eXchange/Sequential Packet eXchange) è un prodotto creato dalla Novell per le proprie reti, di fatto diventato uno standard durante i primi anni '90. In realtà si tratta di due protocolli distinti che però sono così simili da lavorare insieme e formare un unico protocollo. Il protocollo IPX può essere considerato simile a quello NetBIOS/NetBEUI infatti anch'esso prepara pacchetti di dati e li inoltra semplicemente nella rete, non curandosi che il destinatario sia connesso, se li abbia ricevuti integri né, tantomeno, se li abbia effettivamente ricevuti. Per questo motivo è stato affiancato ad esso SPX che invece è in grado di assolvere queste in-

formazioni e di identificare uno specifico computer nella rete attraverso il nome dello stesso e un particolare indirizzo memorizzato nell'hardware di rete al momento della costruzione. Si tratta di un robusto e solido protocollo di rete il cui rappresenta un unico svantaggio di nn possedere il controllo centrale sui nomi dei computer connessi, e quindi passibile di conflitti di rete pur se remoti. Offre la possibilità di interfacciare diversi segmenti di rete tra loro attraverso apparecchiature hardware dette router in grado di gestire questo protocollo e di comunicare con reti Novell molto diffuse in ambienti gestionali

>> Protocollo AppleTalk

Questo protocollo è stato studiato da Apple per la messa in opera di reti Macintosh. L'assegnazione di un indirizzo AppleTalk a un determinato nodo avviene dinamicamente, nel momento stesso dell'avvio del computer, il sistema sceglie l'indirizzo autonomamente e invia sulla rete una richiesta di conferma.

Se nessun altro computer risponde, l'indirizzo scelto viene autonomamente assegnato per la connessione corrente. Se invece l'indirizzo scelto è già stato assegnato,il computer riceve la risposta segnalante l'errore da parte di quello che per primo ha ottenuto l'indirizzo in questione e di conseguenza ne prova un altro fino a quando nn ne trova uno libero.

Il tutto chiaramente senza un intervento dell'amministratore di rete o del gestore del computer.

Ogni indirizzo di rete AppleTalk viene associato all'hardware di rete del computer a cui è stato assegnato.

Nel momento dell'invio dei dati il computer controlla se nel proprio database temporaneo se esiste già un associazione indirizzo-hardware simile a quella ricevuta se dovesse essere così riconosce il computer in questione e velocizza l'operazione.

Al di là di tutta questa semplicità di utilizzo esistono dei limiti nel protocollo AppleTalk infatti non ha avuto grande diffusione al di fuori di reti Macintosh. Innanzi tutto il particolare File System adottato da apple rende difficoltoso lo scambio di file da un sistema Apple a un sistema non Apple .

In secondo luogo, il fatto che Apple talk fosse un protocollo proprietario di Apple e quindi ha tenuto lontani i programmatori dai suoi segreti precludendone quasi l'accesso da parte di tecnologie esterne. Oggi le specifiche tecniche sono rese visibili liberamente proprio con lo scopo di invogliare i programmatori...

>> La rete TokenRing

La rete Token-Ring nasce da studi effettuati dalla IBM,e risulta essere la più veloce rete informatica al momento disponibile.

Il nome Token-Ring deriva dalla struttura particolare dei collegamenti, cioè un anello (in inglese Ring) e dalla tecnica di trasmissione dei messaggi.In un anello di connessione viaggiano diversi pacchetti detti token che indicano un particolare stato: libero o impegnato.

Quando un computer connesso alla rete deve trasmettere dei dati,aspetta fino a quando nn riceve in ingresso un token libero che in pratica significa che nn trasporta dati. Non appena individuato questo token lo sostituisce con un token impegnato seguito dal pacchetto di dati da recapitare che così prende il circolo nel flusso di rete. Se il pacchetto di dati,compiuto l'intero percorso, torna al computer che lo ha inviato questo lo elimina dal flusso, rimette al suo posto un token libero e aspetta di



nuovo il suo turno per trasmettere, contrassegnato dal token libero successivo.

Il risultato quindi ovvio è che in una rete Token-Ring la consegna presso il destinatario dei pacchetti viene sempre garantita in quanto essi vengono sempre ritrasmessi fino a esito positivo, cioè fino a quando nn vengono eliminati dal flusso di rete dal computer del destinatario che li sostituisce a sua volta da token liberi.

Questo sistema unitamente alla qualità dei pacchetti utilizzati (si pensi ai fasci di fibre ottiche), fanno delle Token-Ring reti ad alte prestazioni, adottate quando la mole di dati da trasmettere è notevole.

LE TIPOLOGIE DI RETE

LE RETI A MAGLIE

Sono reti in cui ogni singolo nodo è collegato con molti altri nodi, al limite con tutti. In una rete distribuita i messaggi vengono inoltrati da un nodo all'altro scegliendo uno dei molti percorsi disponibili. La scelta del percorso può avvenire in modo dinamico, secondo le condizioni di traffico della rete. Si noti che in ogni caso il percorso di un messaggio impegna solo un sottoinsieme dei nodi disponibili, e ciascuno per un tempo limitato.

LE RETI A STELLA

Sono basate su un nodo centrale (detto hub) al quale sono connessi tutti gli altri nodi periferici. La comunicazione tra due nodi viene mediata sempre dal nodo centrale.

LE RETI A BUS

Nelle reti a bus tutti i nodi sono collegati a un cavo lineare (bus), come gli affluenti di un fiume, mediante delle diramazioni cui sono collegati i computer. In questo tipo di rete tutti i nodi condividono un medesimo canale di trasmissione, ed inoltre ogni messaggio viaggia sempre in tutte le direzioni.

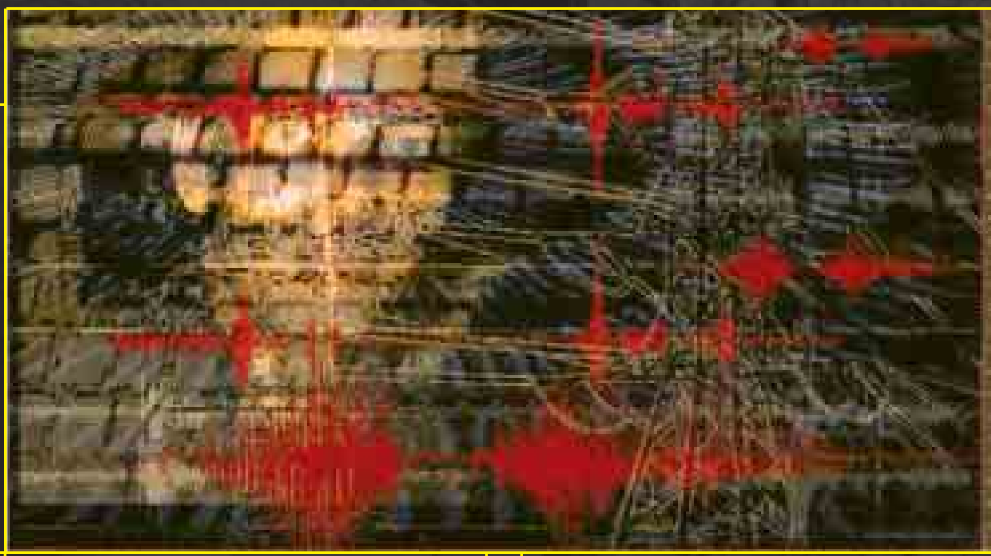
LE RETI AD ANELLO

Le reti ad anello infine, sono costituite da una serie di nodi interconnessi in modo da formare un anello chiuso.

Ethernet: E' La tecnologia più diffusa per realizzare LAN. Fu sviluppata da un giovane ricercatore, Bob Metcalfe, che aveva ricevuto il compito di trovare un modo per collegare tra loro le stazioni di lavoro ALTO, i primi computer basati su icone e finestre (altra geniale invenzione nata al PARC e diffusasi solo dieci anni più tardi con la commercializzazione del primo Macintosh da parte della Apple).

ANCHE I PINGUINI "PIANGONO"...

Come eludere il servizio logging su una macchina Unix-like



Entrare in un PC con sistema Unix senza lasciare traccia? Vi spieghiamo come con la solita preghiera: non fate c***e...**



>>Descrizione e funzionamento

Se siete dei neofiti di Linux, potreste non avere familiarità col logging che ora possiamo dire diventato una procedura base nei computer. Cosa è esattamente il logging? E' la registrazione delle informazioni di sistema e viene effettuata mediante syslogd, ovvero il daemon di logging di sistema che rimane in ascolto delle informazioni inviate ad esso dai vari programmi che può scrivere sui log (registri) oppure ignorare a seconda del contenuto del file di config, che gli dice dove scrivere l'apposito file di log.

Il syslogd viene avviato automaticamente nel corso dell'inizializzazione del sistema però c'è un caso in cui questo daemon non è in esecuzione ossia quando il sistema è al livello di esecuzione 1 (utente singolo). Il motivo per cui syslogd non è abilitato al livello di esecuzione 1 è che non è in esecuzione nulla che possa effettivamente dialogare con esso tranne il kernel che però ha un buffer dove vengono salvati messaggi finché syslogd non è attivo. All'avvio syslogd ascolta i programmi in attesa che essi gli inviino messaggi, utilizzando un particolare **socket UNIX: /dev/log**, che è una sorta di pipe aperto a cui i programmi possono, appunto, inviare messaggi che il demone riceve all'altra estremità, che poi va ad elaborare e a scrivere su un file di log o invia a /dev/null.

Il programma syslogd ha numerose opzioni ma nessuna è abilitata di default e la maggior parte potrà non interessarvi. Quelle che seguono sono alcune delle opzioni di uso comune per syslogd:

Opzione Utilizzo
-h Serve ad inoltrare i messaggi che syslog riceve da altri host a un host centrale di logging (richiede -r);

-a <socket> Se eseguite un daemon in un chroot jail cosi si va a specificare la posizione del socket del log. Si possono aggiungere fino a 19 socket di log aggiuntivi.

(Cosa è un chroot jail? E' una semplice sottodirectory da cui un determinato utente non può uscire e che quindi diventa la sua root di sistema e visto che non si può definire una root effettiva tutto ciò limita i danni che qualcuno può fare manomettendo il daemon eseguendolo come se fosse quel utente).

-m <interval> Con questo specificherete una sorta di intervallo tra voci - -MARK- - nel log. Di default esso è di 20 minuti e con un semplice 0 si può disattivare il logging di - -MARK- -.

-l <hostlist> Lo switch -l diciamo, disattiva i nomi lunghi per gli host che vengono elencati. Ad esempio hostlist è un elenco di host separato da due punti.

-r Questa opzione dice a syslog che può ricevere messaggi (mette syslog vincolato alla

porta 514 come è definito in /etc/services, senza questa voce syslog non si avvierà).

-s <domainlist> Server per effettuare lo strip off dei nomi di dominio elencati, infatti list è un elenco di nomi di dominio separati da due punti.

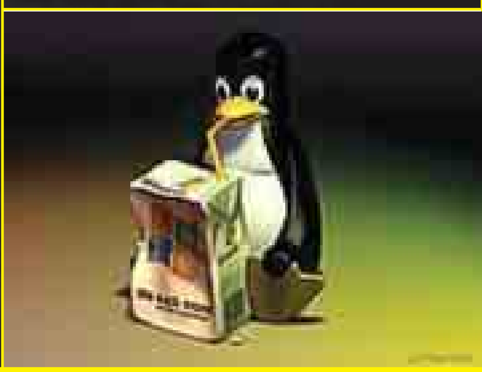
Ci sono chiaramente anche altre opzioni ma servono principalmente per il debug e in condizioni normali non tornano molto utili.

Esiste un evoluzione di questo servizio, chiamato syslog-ng. Si differenzia dal precedente per diverse funzionalità aggiunte, per la possibilità di filtrare i messaggi impostando delle regole e soprattutto per il transito dei messaggi utilizzando TCP e non UDP. Per maggiori informazioni la pagina di manuale di sistema risponderà ad ogni domanda.

>>Elusione del servizio

Come ben si sa non tutto è sicuro al 100% e anche i sistemi di logging rientrano in questa categoria.

Prendiamo ad esempio syslogd. Come spiegato sopra syslogd scrive su diversi files impostati in un file di configurazione: quelli in /var/log e i tre files wtmp, utmp e lastlog. Questi ultimi sono particolari rispetto agli altri e per prima cosa andranno trattati in modo diverso. Cominciamo dall'inizio. Dovremo pulire i files in /var/log da una stringa da noi scelta e, per farlo, dovremo essere root, poi creeremo un file temporaneo eliminando le linee di logs in cui è presente la parola interessata, sfruttando ad esempio grep, wc e awk, compiendo l'operazione un numero di volte pari ai logfiles presenti nella directory. Sostituiremo i files originali con quelli modificati rimpiazzando la data con quella iniziale (es. touch -r).



Il passo successivo sarà cercare logs presenti in altre locazioni. Per questo analizzeremo i files di configurazione del demone di logging (per le problematiche relative all'interpretazione dei confs vi rimando al manuale di sistema) ed utilizzeremo la procedura precedentemente spiegata anche per gli altri elementi trovati.

Infine restano questi "strani" wtmp, utmp e lastlog. La loro notazione è diversa dalle altre plaintext e per questo va ricercata la stringa da eliminare all'interno del file, togliendo soltanto quella e lasciando il resto invariato, mentre negli altri la prassi era quella di eliminare tutta la linea.

Sulla rete si possono trovare numerosi tools da scaricare per analizzare il codice sorgente. Qui non spiegheremo come realizzarne uno ma tratteremo la parte riguardante il funzionamento.

Successivamente resta la possibilità che un amministratore di sistema abbia dislocato logs in posizioni non elencate nelle configurazioni e quindi sarebbe bene utilizzare programmi di ricerca files analizzandone il contenuto.

Sarebbe bene non attuare questa funzione ogni volta poiché aumenta notevolmente il carico della cpu e dell'hard disk e renderebbe l'operazione "pericolosa" se si vuole essere ben nascosti. Per la pulizia dei possibili files trovati, essendo copie o testi generati automaticamente, dovrebbe essere sufficiente utilizzare il ciclo già spiegato.

Una volta puliti i logs sorge una difficoltà: modificando questi files il syslogd smette di scrivere nell'output file e il demone necessita di essere riavviato. I problemi sono due: il primo è il fatto che riavviandolo scriverà nei logs il riavvio del demone e il secondo i MARKs.

Syslogd dal momento in cui viene avviato scrive nei logs un messaggio che per default è ogni 20 minuti, del tipo "- -MARK- – Hostname Data Ora etc" e che si ripete all'infinito fino a un riavvio del demone.

Questa procedura necessita di essere compiuta simultaneamente per risolvere ogni problematica nello stesso momento. Per quanto riguarda la scrittura del restart basta un semplice modulo del kernel che



vada a intercettare la chiamata, mentre simultaneamente uno script va a modificare le linee dei MARKs fino al riavvio precedente del demone.

Queste verranno modificate prendendo in considerazione l'orario in cui viene eseguita l'operazione, proseguendo a ritroso a seconda del tempo di intervallo impostato per i MARKs, ripetendolo per ogni linea.

Dopo aver simultaneamente cambiato i MARKs, caricato il modulo e riavviato il demone possiamo rimuovere il modulo e considerare finita l'operazione.

Per quanto riguarda syslog-ng il procedimento da attuare è lo stesso, cambiando soltanto l'interpretazione del file di configurazione in modo tale da analizzare la nuova sintassi.

Ovviamente il tutto non è così semplice come può sembrare a parole, ma con una giusta analisi si può realizzare un applicativo in grado di fare tutto ciò che è stato spiegato in questa sezione. Con questi passaggi, sulla macchina presa in esame non dovrebbe rimanere alcuna traccia di una possibile intrusione o di un possibile lavoro nascosto di un amministratore di sistema.

r. & d.

?

Host: Computer al quale possono collegarsi in modo più o meno ramificato altri computer.

Script: Si tratta di un codice che può essere eseguito direttamente da un programma. Quest'ultimo in grado di interpretare il linguaggio con cui è stato realizzato lo script.

EFFETTI DAVVERO "SPECIALI"

Effetti speciali?

Grazie pinguino: Linux ed effetti digitali sono un connubio che ha dato risultati strabilianti,

Molti si saranno stupiti guardando il Signore degli anelli "la compagnia dell'Anello", il primo film di una trilogia girata dal regista Peter Jackson. Stupore derivante dal realismo degli effetti speciali, ma chi bazzica questo settore affascinante dell'informatica non si sarà tanto stupito per la qualità degli effetti, in fin dei conti anche il team che aveva lavorato al seguito de "La Mummia" aveva messo in mostra elaborazioni digitali veramente notevoli.

Quello che ha stupito è stata la quantità di effetti. In tre ore di film quasi un'ora di soli effetti speciali per un totale di circa 1.200 effetti distribuiti su tre film. La prima domanda che uno si sarà posto è: come hanno fatto?

Per eseguire il rendering di alcune scene, come quella nella miniera dei nani e della lotta successiva con i goblin, era necessario ricorrere a processori di potenza inusitata e anche disponendo di tutta quella potenza risultava difficile credere che fosse possibile raggiungere un tale livello di definizione. Eppure è stato possibile… usando come sistema operativo proprio Linux.

In realtà per rifinire la prima delle tre puntate che compongono la trilogia sono stati utilizzati "solo" 16 server dual processor SGI 1200 equipaggiati proprio con Linux Red Hat. Ogni singolo processore è costato 3,400 dollari, tutto sommato una cifra abbordabilissima. La grande novità è stata proprio quella di usare un sistema open source per ottimizzare le operazioni di rendering. La società che ha sviluppato il SiÉ



degli Anelli ha sede a Wellington, capitale della Nuova Zelanda, si tratta della Weta-digital, una azienda salita alla ribalta degli effetti speciali per aver realizzato probabilmente il miglior film di animazione digitale mai apparso sullo schermo: Shrek. Al di là della storia, quello che stupiva nel film e forse stupisce ancora, è la capigliatura della principessa Fiona, uno dei personaggi protagonisti, costituita da capelli che sembrano veri, setosi, non un parruccone di plastica appiccicato in testa.

Per renderizzare tutta questa meraviglia evidentemente ci sono voluti sforzi enormi, ma Red Hat ha agevolato non poco la realizzazione.

Sempre in ambiente Unix si è realizzato un altro capolavoro dell'animazione digitale in 3D: Final Fantasy.

Infatti il team di sviluppo ha impiegato uno dei più potenti software di modellazione delle superfici: Maya e precisamente la versione 3.0.

Maya è un software completamente integrato che racchiude molte funzionalità, non è superiore a Lightwave nella modellazione pura, tanto per fare un esempio, ma nella realizzazione di effetti in 3D dinamici per il cinema è assolutamente imbattibile.

Tra l'altro Maya è stato sviluppato anche per Mac OS X e per Windows, tuttavia dà sicuramente il meglio di sé in ambiente Unix, quindi Mac e PC equipaggiati con Linux sono sensibilmente avvantaggiati rispetto ai sistemi Windows.

? **Primitive:** sono le forme geometriche di base: sfera, quadrato, piramide, ecc. che si combinano tra loro e poi vengono modellate fino ad ottenere la morfologia desiderata…

>> Maya

probabilmente la Suite dei sistemi di modellazione e rendering 3D, nonché di animazione. Sviluppato da Alias Wavefront è un software professionale nelle prestazioni e nel prezzo , circa 17.000 dollari, anche se recentemente è stata messa in commercio una versione più economica per il pubblico casalingo. Consente di agire liberamente sulla programmabilità e sulla gestione totale del Work-Flow di lavorazione. Sul sito della Alias/Wavefront **(www.aliaswavefront.com)** è possibile scaricare una demo che è perfettamente funzionante ma che stampiglia dei watemark belli evidenti sui rendering e sui salvataggi.

>> Cinema 4D



La Maxon, notissima casa tedesca specializzata nella produzione di software 3D, ha dalla sua uno dei migliori applicativi in assoluto: **Cinema 4DXL.**
Le nurbus (primitive) di Cinema 4D permettono un grande livello di modellazione, inoltre presenta una funzione "history" in cui si tiene traccia di tutte le operazioni eseguite ed in cui è possibile tornare indietro a ritroso se ci si accorge di avere commesso degli errori.
Ottimo il livello di interazione con la fase finale di rendering che può essere ricalibrata su tutto il modello in lavorazione o solo su una parte dei poligoni.
La parte in cui il programma dà il meglio di sé è indubbiamente l'animazione 3D che rappresenta un po' la "killer application" di Cinema 4D.
La demo si scarica dal sito **www.maxon.net.**

Li faccio io



per una piattaforma che non finisce di stupire...

>> Lightwave



Si parla di programmi top e Ligthwave vanta un primato nella modellazione statica. Se si vuole creare un progetto statico si tratta del programma probabilmente migliore in assoluto che consente di intervenire con grande precisione sui poligoni delle primitive e di modificarli e distorcerli a piacimento. Unico problema l'interfaccia quasi completamente testuale che può sgomentare i neofiti abitati a delle belle interfacce ricche e colorate. Tuttavia una volta padroneggiata, la struttura di lightwave si dimostra facile e funzionale consentendo di ottenere risultati davvero strabilianti. Si può scaricare dal sito **www.newtek.com.**

>> Poser



Se volete realizzare delle figure umane Poser consente di ottenere ottimi modelli senza troppa fatica.

Si tratta di un programma specializzato nelle creazioni di figure umane, con poche primitive disponibili e una grande quantità di librerie dove sono disponibili personaggi 3D già belli e pronti solo da vestire e personalizzare. La demo si trova sul sito **www.curioslab.com.**

>> Se li volete gratuiti...

Chiaramente i programmi si possono anche scaricare "gratuitamente". Alcuni indirizzi utili sono:

-http://fb.provocation.net/www.flasback.net/~krano/a.htm
-http://www.astalavista.com/
-http://www.elitehackers.com/main.shtml
-http://www.crackstore.com/.

UNO SCHELETRINO ANIMATO

Tanto per rinfocolare le polemiche sull'uso gratuito dei teschi che viene fatto in questa rivista (a dire il vero in questo numero abbiamo abbandonato il tema almeno in copertina) vi forniamo un piccolo tutorial per realizzare uno scheletro animato per arricchire il vostro sito web o per semplice diletto. Per eseguire l'operazione utilizziamo Poser, il programma più funzionale per animare personaggi umani o, semplicemente, la loro "infrastruttura".

1 Scegliere il modello

Bisogna selezionare il nostro scheletro. Poser ce lo fornisce bello e pronto nella libreria "Figures>additional figures"

2 Selezionare una posa

La nostra missione è quella di animare lo scheletro, anzi, per essere più precisi, lo vogliamo fare salutare, conviene partire da una posa di partenza che sia sufficientemente vicina a quella che vogliamo fargli assumere con il movimento. Per fare ciò selezioniamo la sezione "Poses" e scegliamo quella che fa al caso nostro…

3 Impostare il movimento

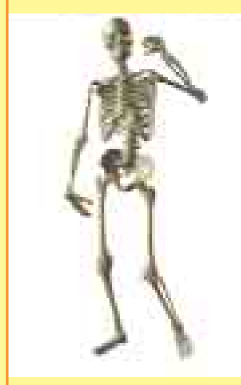
Ai piedi della nostra figura abbiamo una barra che tiene il conteggio dei frame dell'animazione che andiamo ad impostare. Lo 0 corrisponde al punto di partenza. Ora dobbiamo avanzare la freccia che si trova sulla barra fino al frame in corrispondenza del quale si compie il primo movimento.

La portiamo a 10 e poi impostiamo il movimento che ci interessa. Per eseguire la prima fase del saluto, dobbiamo fare oscillare la mano agendo sulle ghiere alla destra dell'area di lavoro che spostano in ambiente tridimensionale gli oggetti. Basta selezionare la mano con il cursore e poi agire in modo combinato su Bend, Side Slide e Twist fino a portare il braccio al punto desiderato

4 L'animazione

Ora selezioniamo il frame 20 e spostiamo allo stesso modo il braccio dall'altro parte facendogli compiere un mezzo cerchio. Il saluto è completo, per renderlo ancora più efficace possiamo selezionare il frame finale, 30, e tornare al punto di partenza.

Il nostro teschio che saluta è pronto basta selezionare Animation>MakeaMovie e scegliere le opzioni di compressione e formato preferite e il gioco è fatto!









Il porno che ti spia



Naturalmente nessuno di noi si è mai sognato di visitare un sito porno (vero?), ma si dice che chi lo faccia riceve poi decine di e-mail con offerte xxx...

Magari vi sarà capitato di guardare di sfuggita un sito a luci rosse, magari di nascosto, chiusi in uno sgabuzzino con il PC dotato di opportuna prolunga, la luce spenta e l'ambiente irradiato solo dei bagliori del video. Avete magari anche pensato che nessuno potesse scoprire queste vostre navigazioni "solitarie". Sbagliato, la brutta notizia è che lo sanno tutti perché i siti pornografici sono dei sensazionali mezzi di monitoraggio dell'utenza internet.

>> Annunci erotici a go go

Non si capisce per quale motivo, ma dopo aver navigato su siti porno si cominciano a ricevere decine di mail con offerte piuttosto equivoche di abbonamenti gratuiti a siti erotici, prezzi scontatissimi su oggetti che neanche nei peggiori sexy-shop acquisteremmo mai ed altra robina simile. Se qualcuno dovesse scaricare la posta al vostro posto, magari in ufficio, certo la brutta figura è in agguato.

Perché riceviamo questa notevole quantità di spazzatura? Semplice, perché, grazie ai "bad cookies", siti come **Doubleclick.com** (uno dei più grossi tracker mondiali) sono in grado di carpire anche questa informazione mentre navighiamo ignari. Per evitarlo dovremo prestare attenzione ad alcune cose:

1. Non lasciare mai l'email in nessun sito porno.

2. Se usiamo software come ICQ, MSN Messenger o simili, non inserire mai il nostro indirizzo di posta elettronica, al limite potremo crearne uno "di servizio", utilizzando Hotmail o altri siti simili.





3. Non rispondere mai adun messaggio di spam e non cercare di contattare il webmaster del sito che lo ha inviato. Come solo risultato avremo quello di confermare che il nostro indirizzo di email è attivo e verremo sommersi da email spazzatura.

>> Altre avvertenze

Il "tracker", in questi casi, tiene traccia dei gusti dell'utente, ne controlla la navigazione, annotando i siti ai quali ci si connettete, riesce a controllare cosa si acquista in rete ed un sacco di altre informazioni sui nostri gusti. Potenzialmente potrebbe anche carpire informazioni riservate come password o dati inseriti nelle form. Ma conoscendo i nostri gusti, il giorno dopo sarà in grado di fornirci una scelta già bell'e pronta di quel che ci piace. Tanto, siamo schedati...

Per proteggerci da questo tipo di pericoli abbiamo alcune armi:

1. disabilitare i cookies agendo sulle impostazioni del browser.

2. proteggerci con un software in grado di abilitare/disabilitare la ricezione di contenuti potenzialmente dannosi da Internet (es. Norton Internet Security 2001).

3. cancellare i cookies una volta terminata la sessione di navigazione.

>> Software anti pop-up

Altra pratica invasiva di molti siti, specie quelli porno, è l'apertura di decine di pop-up che impediscono fisicamente all'utente di abbandonare il sito bloccandolo per diversi secondi.



Per eliminare e prevenire l'apertura di queste fantomatiche finestre torna utile Morpheus Pop Up Ad Killer, un utile software shareware che si può scaricare facilmente all'indirizzo **http://www.esdpc.com** e che "uccide" le finestrelle invasive.

QULCUNO C'E' RIUSCITO? DITELO!

NEWBIE

ARRIVA IL NUOVO SISTEMA DI CODIFICA DIGITALE



LA GRANDE SFIDA DI TELEPIU'

Seca 2 a prova di hackers?

In Italia hanno da qualche giorno lanciato il nuovo sistema di codifica digitale, il Seca 2, l'intento è di debellare le smart card pirata. Ci riusciranno?

Tele+ ha lanciato la sfida a quei 2 milioni di possessori di smart card pirata che ne mortificano il bilancio. Dopo aver passato gran parte della stagione a cambiare frequenze prima delle partite, per scoraggiare i pirati occasionali o quelli che acquistano le schede da fantomatici trafficoni da bar, ora hanno deciso di affrontare a muso duro la comunità di hacker che, dalla rete, diffonde notizie atte a scardinare i sistemi di codifica digitale. Il tutto dovrebbe avvenire con il lancio di Seca 2 e la manovra interessa tutte le aziende del gruppo Tele + che trasmettono in Polonia, Francia, Spagna ecc.

>> Il testo "sacro"

Proprio in questi giorni è avvenuta la sostituzione, in Italia, delle vecchie schede con le nuove che supportano il Seca 2 e che con buona probabilità non saranno facilmente "leggibili", contenendo nuove istruzioni e una crittatura più drastica dei dati. Ma facciamo un piccolo passo indietro. Fino a qualche mese fa chi avesse voluto fabbricare schede pirata trovava un gran numero di documenti in rete a partire dal "testo dei testi": Wafer4Dummies, 109 pagine, scritto da Klontz che descrive passo passo cosa serve per ricevere una trasmissione via satellite in chiaro con l'uso di una scheda pirata.

Ma esistono altri "testi sacri", fra questi, un'altra enorme enciclopedia, riservata a chi ha conoscenze già avanzate, è senza dubbio l'imponente "Prontuario del Seka" di IperSat. A pochi mesi dal lancio in Spagna del sistema Seca 2, sembra però che non si sia ancora trovata la soluzione per decrittarlo. Non ci sono riusciti gli hacker iberici che ci lavorano da un po', né tanto meno quelli italiani, almeno questo è quello che sembra consultando i canali abituali, oppure i forum: http://satnet.caltanet.it/forum/yabb.pl.

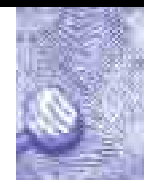
Di fatto gli ingegneri di Tele+ hanno fatto pubblicare comunicati stampa anche un po' provocatori in cui dichiarano "di sbellicarsi dalle risa" leggendo le notizie che qualcuno è riuscito a decrittare il Seca 2.

>> Cosa sta succedendo

La comunità underground incassa ma sta pensando a una rivincita clamorosa. Quanto ci vorrà a far saltare il Seca 2? Due mesi? Forse, un anno. Cosa succederà non possiamo saperlo. Nel frattempo girano in Rete i primi file che mettono in chiaro NDS, il sistema di codifica di Stream. Non è escluso che se diventasse impossibile tenere "aperto" il nuovo SECA, la pirateria riverserà i propri sforzi su NDS per vedere col decoder Italtel di Stream gli stessi canali disponibili con il Goldbox di Tele+.

SCHEDE

LE SCHEDE



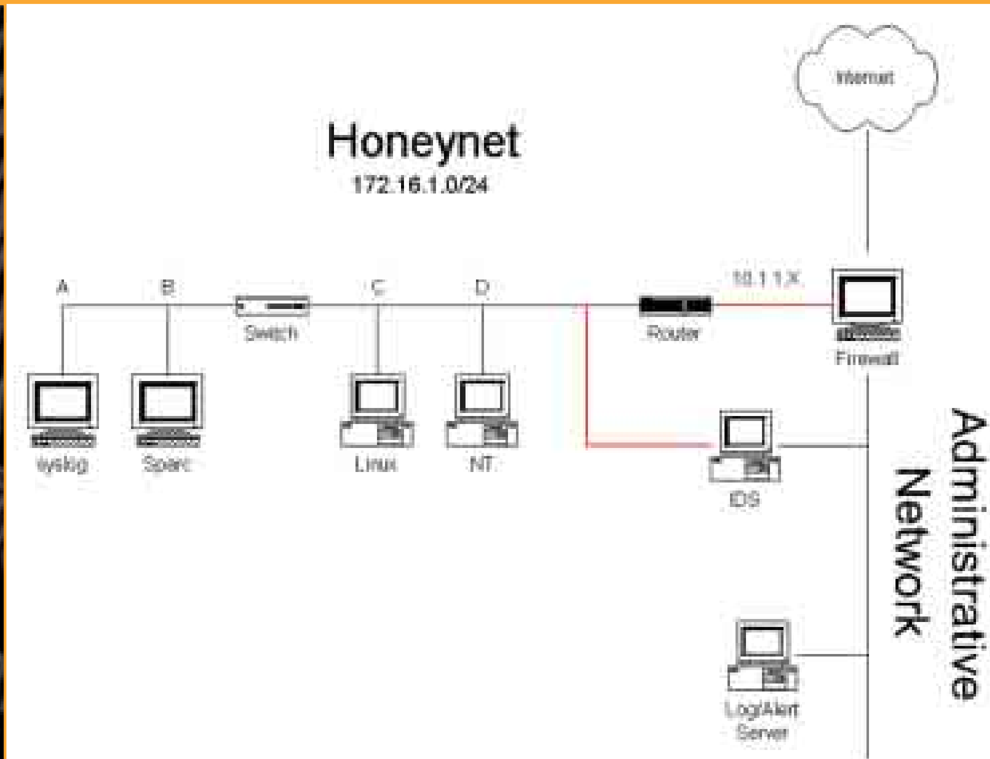
Vale la pena, a questo punto, di delineare quello che è stato lo scenario delle schede fino ad oggi. Prima dell'avvento del Seca 2 in commercio esistevano (o meglio esistono ancora ma forse non potranno servire per aggirare Seca 2) almeno 3 tipi di carte pirata diverse: le Wafer card (all'estero sono chiamate Piccard 1 o, più semplicemente, Piccard, ma pare siano le meno efficienti), le Piccard 2 e le Fun Card, di gran lunga le meglio. Sono quelle che molto più comunemente sono chiamate "schede pirata". Tutte sono composte da un circuito stampato che collega una eeprom e una pic, per poi terminare all'altro lato della scheda con i contatti che replicano fedelmente quelli di una scheda (smart card) originale. Le tre schede si differenziano fra loro per l'hardware che montano e, di conseguenza, per la memoria a disposizione "on board". Ognuna di queste tre schede ha un corrispettivo plastico, che cioè ha integrato i chip in modo che non siano estraibili fisicamente dal supporto: sono meno versatili ma esteticamente più accurati; eccezione fatta per il logo della Pay TV non presente su Gold Card, Silver Card e Purple Card. Che siano in formato plastico o meno, sulle pic di tutte le carte vengono caricati i software che emulano le smart card originali mentre sulle eeprom occorre caricare i codici operativi veri e propri.

ERIGERE UN “MURO” CONTRO GLI ATTACCHI IN RETE



Honeynet: la rete da attaccare

Cos’è un honeynet? Semplice un honeypot! Vabbé leggete l’articolo che è meglio...



Nel numero 2 abbiamo fatto un’intervista a Lance Spitzner responsabile del progetto Honeynet. Ma cos’è un’Honeynet? E’ un tipo di honeypot specifico per la ricerca. Un honeypot è rappresentato da una risorsa il cui valore è quello di essere oggetto di scan, essere attaccato o compromesso. Il suo princupio è quello di trarre in inganno un possibile attacker o la rilevazione degli attacchi.

Di solito sono sistemi singoli che emulano altri sistemi, oppure emulano servizi conosciuti o vulnerabilità, o creano ambienti jailed. Alcuni eccellenti esempi di honeypot includono Specter (http://www.specter.com), Mantrap (http://www.recourse.com/product/ManTrap/), o il nuovo Deception Toolkit (http://www.all.net/dtk/). Una honeynet differisce dagli honeypot tradizionali per il suo fine puramente di ricerca. Questa non è una soluzione migliore rispetto agli honeypot tradizionali piuttosto ha scopi differenti. Il valore di una honeynet piuttosto che trarre in inganno o rilevare un attacco è quello di trarre informazioni su una possibile minaccia.

Ci sono alcune differenze rispetto ad un honeypot classico: non si tratta di una singola macchina ma di una rete di sistemi. Questa rete è posta dietro un device a controllo di accesso, di solito un firewall, dove tutto il traffico in entrata ed in uscita è controllato e catturato.

Le informazioni catturate vengono successivamente analizzate per conoscere i tools, le tattiche e i motivi della comunità dei blackhats. Le honeynets possono utilizzare più sistemi operativi allo stesso tempo come Solaris, Linux, Windows NT, i routers Cisco router, gli switch Alteon, etc. Questo crea un ambiente di rete quanto più simile è possibile ad una rete in produzione.

Inoltre, avendo a disposizione differenti sistemi operativi con differenti applicazioni come un DNS Server su Linux, un Information Server su piattaforma Windows, un RDBMS su Solaris, possiamo conoscere tool e tattiche differenti. Alcuni blackhats ricercano sistemi operativi specifici, applicazioni o vulnerabilità. Avendo a disposizione una varieta' di sistemi operativi e di applicazioni, siamo in grado di rilevare con precisione i trend di crescita di un determinato fenomeno. Tutti i sistemi che rappresentano una honeynet sono sistemi di produzione standard; si tratta di sistemi operativi reali e di applicazioni, le stesse che possiamo trovare su internet tutti i giorni. Niente e' emulato e non viene fatto nulla per rendere un sistema meno sicuro.

I rischi e le vulnerabilità scoperte con una honeynet sono le stesse che esistono in molte aziende oggi.

E' possibile prendere un sistema in produzione e spostarlo nella Honeynet per conoscerne i punti deboli.

Anche se una honeynet puo' essere utilizzata come un honeypot tradizionale per rilevare i tentativi di accesso non autorizzati, di solito mantenere una honeynet richiede piu lavoro rischio e amministrazione.

>> I requisiti principali

Due requisiti principali di una honeynet sono il controllo dei dati e la cattura dei dati, se uno di questi due fallisce avremo problemi sulla nostra honeynet.

Il controllo dei dati serve a mitigare i rischi; una volta che una macchina presente sulla honeynet è stata compromessa non dobbiamo rendere in grado l'attacker di utilizzare questo sistema per danneggiare altre risorse presenti su internet.

Un terzo requisito potrebbe essere quello di collezione dei dati ma solo per le organizzazioni che possiedono honeynets multiple in ambienti distribuiti. In caso di honeynets multiple distribuite logicamente o fisicamente nel mondo, i dati devono essere conservati in modo centralizzato per aumentare il valore delle informazioni catturate. Vediamo in dettaglio come è strutturata una honeynet e come funziona :

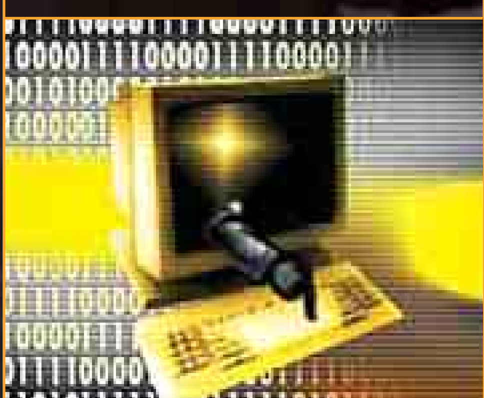
Come possiamo notare dalla figura 1 il firewall separa la honeynet in tre reti Honeynet, Internet e rete di amministrazione; ogni pacchetto che entra o esce dalla nostra honeynet deve passare per il firewall ed il router.

Il firewall rappresenta il nostro device primario per il controllo di accesso dei pacchetti in entrata ed in uscita mentre il router viene utilizzato per rafforzare questo tipo di controllo di accesso proteggendo la nostra honeynet da attacchi di tipo spoofing, Denial of service, ICMP.

Posizionare un router aggiuntivo rispetto al firewall ha lo scopo di rendere l'ambiente quanto piu' realistico è possibile. Di solito su questo tipo di infrastruttura di tende a bloccare il numero massimo di connessioni in uscita dalla honeynet ad un massimo di 5. Questo scopo può essere raggiunto con un qualsiasi tipo di firewall, sia esso Firewall-1 di Checkpoint, IPFILTER o IPTABLES di Linux.

La cattura dei dati consiste nella cattura dei dati; per fare questo possiamo utilizzare il firewall o il nostro IDS.

Il sistema IDS ci può dare informazioni dettagliate sul tipo di attacco e può registrare tutte le informazioni che passano sulla rete. Un ulteriore livello di logging è rappresentato dai log dei sistemi stessi spediti ad un syslog centralizzato tramite connessioni criptate.



>> C'è honeynet e honeynet

Un'ulteriore evoluzione delle honeynets in questo momento è rappresentata dalle virtual honeynets: si tratta di un unico sistema fisico che utilizzando un emulatore di pc come VMWARE (http://www.vmware.com) rende in grado di avere un sistema operativo reale a scelta tra Linux, Openbsd, Freebsd, Solaris, Windows e risponde a tutti i requisiti di una honeynet.

In questo modo otteremo anche un minor costo di gestione e di



amministrazione. Un altro interessantissimo strumento di virtual honeynet è honeyd di Niels Provos (reperibile alla url: http://www.citi.umich.edu/u/provos/honeyd/).

Honeyd è un daemon che crea dei virtual hosts su una rete. Gli hosts possono essere configurati per avere dei servizi fittizi e emulare diversi sistemi operativi.

E' possibile eseguire ping e tracerouter sulle macchine virtuali. In questa breve panoramica abbiamo visto come una honeynet sia un interessantissimo strumento di ricerca per conoscere sia i punti deboli della propria rete sia per conoscere nuovi attacchi e nuove vulnerabilità.

Dobbiamo però tenere conto che una honeynet e' uno strumento delicato che richiede costante manutenzione e lunghi tempi di analisi.

Se da una parte una honeynet può essere compromessa in 30 minuti l'analisi di un sistema compromesso può anche richiedere 30 40 ore. In definitiva una honeynet non risolverà i nostri problemi di security ma, al contrario li aumenterà dandoci in cambio un mare di informazioni utili.

?

Solaris: Sistema operativo per la Rete basato su Unix, come Linux, e sviluppato dalla Sun Microsystem.

Stringa: Serie di caratteri collegati, come "UsareInternet senzafatica". Le stringhe accettano tutti i tipi di caratteri: lettere, cifre e simboli di punteggiatura.